Cybersecurity (CYBR)

CYBR 2700. Information Security Fundamentals. (3 Credits)
Prerequisite(s): IT 2600 or CS 2600; (IT 1600 recommended)
Explores introductory information and cybersecurity concepts: security technologies, methodologies, and tools. Includes security models, risk assessment, threat analysis, attack types, encryption technologies, security implementation, access controls, business continuity, and security policies. Discusses current topics, trends, and career opportunities in information security. Includes lab assignments covering information security principles.

Software fee of $24 applies.
Lab access fee of $45 for computers applies.
Canvas Course Mats $49/Cengage applies.

CYBR 2800. Computer Forensic Fundamentals. (3 Credits)
Prerequisite(s): INFO 1120 or IT 1600 or CS 1400 or CJ 1010
Explores procedures for identification, preservation, and extraction of electronic evidence. Emphasizes auditing and investigation of network and host system intrusions, analysis and documentation of information gathered, and preparation of expert testimonial evidence. Examines forensic tools and resources for system administrators and information system security officers. Includes ethics, law, policy, and standards concerning digital evidence. Includes hands-on learning and a research paper or project.
Lab access fee of $45 for computers applies.
Canvas Course Mats $49/Cengage applies.

CYBR 3350. Intellectual Property and Cyber Law. (3 Credits)
Prerequisite(s): ENGL 2010 and (INFO 1120 or CS 1030 or LEGL 3000) and University Advanced Standing
Explores the legal and policy issues associated with the Internet and cyberspace. Studies case law, statutes, regulations, and constitutional provisions that affect people and businesses interacting through computers and the Internet. Covers intellectual property (trademarks, copyrights, patents, trade secrets, and unfair competition) and examines legal requirements to create, register and protect intellectual property rights. Focuses on e-commerce, online contracts, cybercrimes, torts, and privacy issues pertaining to technology.
Lab access fee of $45 for computers applies.

CYBR 3700. Ethical Hacking and Countermeasures. (3 Credits)
Prerequisite(s): IT 1510, CYBR 2700, and University Advanced Standing
Pre- or Corequisite(s): IT 3600
Examines advanced information security concepts through an applied viewpoint. Extends the student's understanding of security issues through hands-on application of real-world techniques and use of current security software. Includes legal/ethical issues, use of security tools, network reconnaissance, password/brute-force attacks, firewall configuration, honeypot deployment, intrusion analysis/detection, server hardening, and penetration testing. Provides insight into current trends in advanced security issues.

Lab access fee of $45 for computers applies.

CYBR 3750. Malware Reverse Engineering. (3 Credits)
Prerequisite(s): [(CS 2370 and CS 3100) or (CYBR 2700)] and University Advanced Standing.
Examines advanced techniques used in malware analysis. Focuses on static and dynamic analysis of unknown binaries utilizing reverse engineering tools and procedures. Explores advanced anti-malware analysis processes and anti-reverse engineering methods. Covers advanced obfuscation practices, such as employing packers, and anti-debugging processes.

CYBR 4150. Data Security Analytics. (3 Credits)
Prerequisite(s): CYBR 2700 and INFO 2410 and University Advanced Standing; (INFO 3130 and INFO 3410 recommended)
Introduces students to the concept of data analytics as applied to cyber security. Includes collection, aggregation, data mining, and analysis of various data sources. Utilizes data analytics tools that correlate data in order to identify security events that may go undiscovered by traditional detection and log analysis methods.
Lab access fee of $45 for computers applies.

CYBR 4250. Database Security and Auditing. (3 Credits)
Prerequisite(s): (INFO 3410 or CYBR 3700) and University Advanced Standing
Utilizes theories, scenarios, and step-by-step examples. Provides a strong foundation in database security and auditing. Covers the following topics in depth: the importance of database security in contemporary business environments, security, profiles, password policies, privileges and roles, virtual private databases, auditing, SQL injection, and database management security issues.

Lab access fee of $45 for computers applies.

CYBR 4350. Web and Application Security. (3 Credits)
Prerequisite(s): (CYBR 2700 or CS 2550) and University Advanced Standing
Pre- or Corequisite(s): INFO 3300 or CS 3520
Covers the security of web and mobile applications from offensive and defensive standpoints. Explores common vulnerabilities of web and mobile applications and various tools and techniques for identifying and mapping the attack surface of such applications. Explores various techniques and attack vectors for exploiting security flaws in web and mobile applications. Implements secure coding best practices, defensive architecture, and Content Security Policy to mitigate security flaws and protect the applications, the web client, the communication channel, and the server.
Lab access fee of $45 for computers applies.

CYBR 4450. Internet of Things Security. (3 Credits)
Prerequisite(s): IT 1510, CYBR 2700, and University Advanced Standing.
Covers the architecture of Internet of Things (IoT) systems (devices and applications) and the security of these systems from offensive and defensive standpoints. Addresses common IoT vulnerabilities and threats and explores various techniques/tools and attack vectors for exploiting IoT security flaws. Discusses best practices for securing and hardening IoT systems. Includes offensive and defensive hands-on lab activities covering the hardware, software, applications, and network components of of IoT systems.

CYBR 4550. Threat Hunting and Incident Response. (3 Credits)
Prerequisite(s): CYBR 3700 and Advanced University Standing
Provides students with knowledge and practical skills to hunt down threats within networks and end points and to identify, contain, and recover from intrusions and data breaches. Utilizes a combination of lectures, hands-on labs, and case studies to explain the tactics, techniques, and procedures that are employed by threat actors to achieve their goals. Covers the consumption and creation of Cyber Threat Intelligence (CTI) to enhance detection and response capabilities.

CYBR 459R. Current Topics in Cybersecurity. (3 Credits)
Prerequisite(s): CYBR 2700 and University Advanced Standing
Provides exposure to emerging technologies and topics of current interest in cybersecurity. Varies each semester depending upon the changes in the cybersecurity discipline or to address a focused area within the cybersecurity discipline. May be repeated for a maximum of 9 credits toward graduation.

CYBR 4650. Industrial Control Systems Security. (3 Credits)
Prerequisite(s): IT 1510, CYBR 2700, and University Advanced Standing.
Introduces students to the basics of industrial control systems (ICS) including their architectures, types, and various components. Covers how the components of ICS work together and how Supervisory Control and Data Acquisition (SCADA) are organized and managed. Utilizes a combination of lectures, case studies, and hands-on labs to explain the security of ICS including common ICS vulnerabilities and a variety of attack vectors against ICS and SCADA. Covers best practices for securing ICS and implements countermeasures to protect against cyberattacks explored in class.

CYBR 4700. Enterprise Cybersecurity Management. (3 Credits)
Prerequisite(s): CYBR 2700 and University Advanced Standing
Pre- or Corequisite(s): INFO 3430
Provides perspective of key issues involved in IT activities across the organizational and technical security landscape. Examines management methodologies, staffing, and operational issues. Teaches use of financial analysis and decision-making methodologies to aid investment decisions at the operational, functional, and strategic levels. Illustrates use of risk assessment and contingency planning as applied to business continuity and disaster recovery strategies. Includes the use of Service Level Agreement for managing both internal and external relationships.
Lab access fee of $45 for computers applies.

CYBR 4750. Cybersecurity Capstone. (3 Credits)
Prerequisite(s): CYBR 3700 and CYBR 4350 and (CYBR 4150 or CYBR 4550), and University Advanced Standing
Pre- or Corequisite(s): CYBR 4700
Senior-level, capstone experience course. Enhances student cybersecurity knowledge in a self-directed research or practical project that showcases student's mastery of cybersecurity topics. Provides an opportunity to conduct research and/or implement systems that incorporate topics from previous courses. Requires students to present their work at the end of the semester.

CYBR 4760. Case Studies in Cyber Security. (3 Credits)
Prerequisite(s): CYBR 2700 and University Advanced Standing
Discusses current trends, issues, and global events related to cybersecurity. Includes topics on data breaches, cyber warfare, and emerging threats. Emphasizes the changing and transformative nature of cybersecurity threats, including geographical, institutional, and cultural evolution. Examines real-world examples of the application of cybersecurity principles and requires critical analysis of each case. Hosts guest lecturers from industry to provide students with perspectives on the state of cybersecurity.

Lab access fee of $45 for computers applies.

CYBR 4800. Advanced Mobile Devices Forensics. (3 Credits)
Prerequisite(s): CYBR 2800 and University Advanced Standing
Discusses devices that can store digital information such as cell phones, tablets, digital camera/camcorders, thumb drives and memory cards. Focuses on lab investigations of one or more digital media through image acquisition, data analysis, and assembly of a final written report of findings. Provides opportunities to use multiple software tools in device acquisition and analysis. Covers processes and procedures through mock investigations.
Lab access fee of $45 for computers applies.

CYBR 481R. Internship. (1-6 Credits)
Prerequisite(s): (CYBR 3700 and one 4000 course in Cybersecurity), Department approval, and University Advanced Standing.
Provides opportunities to apply upper-division classroom theory while students work as employees in a job that relates to their careers. Requires the student to meet periodically with a Departmental Internship Coordinator. Determines credit based on the number of hours a student works during the semester and completion of individually set goals. Requires prior written Department Chair approval to apply more than three credits toward a Bachelor of Science Degree in Cybersecurity. May be graded credit/no credit.

CYBR 4850. Digital Forensics Investigations. (3 Credits)
Prerequisite(s): CYBR 2800 and University Advanced Standing
Covers one or more investigations from start to finish. Integrates knowledge and skills from previous CJ, FSCI, and IT courses in this culminating experience.
Lab access fee of $45 for computers applies.