UNDERGRADUATE COURSES OF STUDY

CYBERSECURITY

CYBR 140.NETWORKING LAB
Designed to provide students with an understanding of the principles of computer networks and protocols through hands-on activities and experimentation. Topics include: static and dynamic addressing, building LANS and VLANS using switches, building internetworks using routers, configuring network components to allow or deny access, deploying and evaluating communication protocols using network utilities and server software that are used in present day network infrastructures, and other emerging topics. ***One credit hour.***

CYBR 243.FUNDAMENTALS OF CYBERSECURITY
Designed to provide a holistic overview of the field of Cybersecurity. Topics include security principles and policies, laws and regulations, security assessment and testing, asset protection, basic cryptography, authentication, ethics, malware, computer and network forensics, threat and vulnerability detection and protection, and other emerging topics. Prerequisite: "C" or better in CIS 130. ***Three credit hours.***

CYBR 260.NETWORK AND SYSTEM ADMINISTRATION
This course introduces concepts essential to the administration of operating systems and networks. Topics explored include application installation and configuration, user account management, understanding and management of file systems, file backup and restoration, basic operating system commands (including network related commands) and utilities, task automation using scripting, serial and parallel communication, and other emerging topics. Prerequisite: "C" or better in CIS 130. ***Three credit hours.***

CYBR 343.COMPUTER FORENSICS
Computer devices retain far more information than most people realize. Retrieving this information can provide considerable electronic evidence. Computer forensics is the forensic science discipline of acquiring, preserving, retrieving, and presenting electronic data. This course is designed to provide comprehensive understanding of computer forensics principles. Topics include admissibility and preparation of electronic evidence, e-evidence preservation, chain of custody, examination of computers and digital media including operating systems, graphics files, and email, detecting intrusions, malware and fraud, legal and ethical issues and responsibilities, and other emerging topics. Prerequisite: "C" or better in CYBR 243. ***Three credit hours.***

CYBR 344.NETWORK SECURITY AND FORENSICS
To secure a network, administrators must perform a variety of tasks ranging from giving access authorization to data and equipment, to preventing unwanted access and malicious attacks on data or network components. This course is designed to provide a comprehensive understanding of network security and the network forensic analysis principles used when faced with a security breach. Topics include overview of network topologies, protocols, and infrastructure in the context of network security and forensic analysis, techniques for identifying network security breach incidents and potential sources of digital evidence, techniques for network data acquisition and analysis, legal considerations and documentation of forensic processes and analysis, and other emerging topics. Prerequisites: "C" or better in CIS 240, CYBR 243, and CYBR 260. ***Three credit hours.***

CYBR 345.INTRODUCTION TO CRYPTOGRAPHY
Cryptography is an indispensable tool for protecting information in computer systems. This course is designed to introduce students to the inner workings of cryptographic systems and how to correctly use them in real-world applications. Topics include stream ciphers, pseudo randomness, block ciphers, message integrity, hash functions, authenticated encryption, public-key encryption, and other emerging topics. Prerequisite: "C" or better in CIS 130 and CYBR 243. ***Three credit hours.***

CYBR 346. CYBERSECURITY PLANNING AND MANAGEMENT
This course provides a holistic view of procedures and processes for planning and management of cybersecurity operations in an organization. Topics such as laws and ethics pertaining to information systems security, risk assessment and management, identifying needs for security functions, understanding strengths and weaknesses of available security solutions, developing information security policies, developing plans for the protection and access control of intellectual assets, outlining roles of personnel in planning, managing, and maintaining information security, and developing contingency plans for business continuity, disaster recovery, and incident response after a security violation has occurred will be included. Prerequisite: "C" or better in CYBR 243. ***Three credit hours.***

CYBR 443.SPECIAL TOPICS IN CYBERSECURITY

Designed to provide an in-depth study of topics related to Cybersecurity. Prerequisites: "C" or better in CIS 240, CYBR 243, and CYBR 260, or instructor permission. ***One to three credit hours.***

CYBR 449.CYBERSECURITY CAPSTONE

In this capstone course, students conduct research, and design and implement comprehensive cybersecurity projects in a group environment. An oral defense before an audience of students and faculty is required, and faculty will review a project portfolio. Prerequisite: Instructor permission. ***Three credit hours*.**