Introduction to computer networks, including network protocols, communication paradigms, wired and wireless network technologies, and cyber forensics. Students are introduced to the IT and regulation dealing with computer forensics and cyber security. The various laws and regulations related to cybercrime: intellectual property, user privacy, information assurance, and harmful online content. Third unit introduces ethical frameworks applicable to cybersecurity, sources of applicable law and regulation. The goal is to develop a foundation for further study in cybersecurity.

Prerequisite: C S 2413, MATH 1914, and either C S 2813 or MATH 2513.

This course provides an introduction to the UNIX operating system. Topics include files and directories, electronic mail, security, advanced file systems, network utilities, network file sharing, text utilities, shell programming, regular expressions, UNIX internals, UNIX system administration, UNIX variations, and systems programming. Programming assignments involve the UNIX shell script language.

Prerequisite: C S 2413 and MATH 1914; and C S 2813 or MATH 2513.

This course focuses on hardware (HW) security and covers security and trust issues and vulnerabilities in software applications due to a lack of secure software engineering processes.

Prerequisite: CYBS 3323. This course prepares students to securely develop and operate Internet of Things (IoT) devices considering security and privacy. The course covers concepts of IoT architectures with a focus on security and privacy issues.

F: Fall, Sp: Spring
CYBS 4333  Incidence Response Management  3 Credit Hours
Prerequisite: CYBS 3123. This course provides a comprehensive treatment of cyber incidents and how to manage them, including understanding attacker motivation, attack methods, and the anatomy of the attacks. Additionally, topics related to incidence readiness, remote triage tools, memory analysis, malware analysis, disk forensics, network intrusion detection tools, and others will be discussed. (F, Sp)

CYBS 4473  Network Security  3 Credit Hours
Prerequisite: CYBS 3113. The course deals with understanding all aspects of cybersecurity that involve the network. Topics will include network transport-level security, wireless network security, electronic mail security, IP security, firewalls, VPNs, Secure HTTP, person-in-the-middle attack scenarios, and SSL/TLS and SSH (SP). Learn about various tools for analyzing network data at various levels of the TCP/IP stack and operating security operations centers. (F)

CYBS 4583  Machine Learning for Cybersecurity  3 Credit Hours
Prerequisite: CYBS 3213 and ISE 3293. Various machine learning concepts, deep learning, time-series analysis, data mining, and other machine-learning concepts. Tools and libraries to analyze data sets, build predictive models, and evaluate the fit of the models. Common learning algorithms, including dimensionality reduction, classification, principal-component analysis, k-NN, k-means clustering, gradient descent, regression, logistic regression, regularization, multiclass data, algorithms, boosting and decision trees. Applies concepts to problems. (F, Sp)

CYBS 4883  Cryptography Fundamentals  3 Credit Hours
Prerequisite: CYBS 3213. This course introduces cryptography and its related tools. Specifically, in this course, cryptographic algorithms, protocols, and techniques will be introduced. The course will also introduce students to public key encryption, key exchange protocols, digital signatures, hashing-based encryption, and Data Encryption Standards. This course will also introduce cryptographic implementation in software and web application programming. (F)

CYBS 4953  Operating and Maintaining Cyber Ranges  3 Credit Hours
Prerequisite: CYBS 4473. Students will learn to use and build a cyber range for various assessments of threats and exploits. They will learn to build configurations for different business operations and the formation of red and blue team exercises. Students will have real-world experiences in handling situations without the real-world risk associated with practicing on live production equipment and systems. (Sp)

CYBS 4963  Cybersecurity Capstone  3 Credit Hours
Prerequisite: CYBS 4103 and Senior Standing. Provides the students with an experience to exhibit their knowledge and skills in all areas of cybersecurity. Students will work in small groups to identify and scope a cybersecurity problem and/or challenges. Required to write a proposal about their project and asked to create a work plan to develop solution to solve the problem/challenge. Create a final report and presentation. (Sp)