# CYBERSECURITY (CBY)

**CBY 101: Introduction to Cybersecurity (3 credits)**
The purpose of this course is to explore the evolving crime phenomenon resulting from the technology revolution over the last 60 years. An examination of the unique human-computer relationship will be conducted to develop an understanding of how criminal activity has adopted the use of new technologies to further their criminal activity. Additionally, a review of social constructs relating to high tech criminal activity will be provided.

**CBY 200: Introduction to Digital Forensics (3 credits)**
This course is designed to introduce and explore the basic concepts of digital forensic investigations and analysis. Students will learn the basic terminology and tools utilized in a digital forensic investigation. Students will broaden their knowledge and understanding of what a digital forensic investigator does and the types of skills needed in this field.

**CBY 202: Cyber Governance: Privacy, Ethics, and Digital Rights (3 credits)**
Describes the legal and ethical issues associated with information security including access, use, and dissemination. It emphasizes legal infrastructure relating to information assurance, such as the Digital Millennium Copyright Act and Telecommunications Decency Act, and emerging technologies for management of digital rights. It examines the role of information security in various domains such as healthcare, scientific research, and personal communications such as email. It examines criminal activities such as computer fraud and abuse, desktop forgery, embezzlement, child pornography, computer trespass, and computer piracy.

**CBY 220: Cyber Investigations I (3 credits)**
This course prepares students with the knowledge and skills necessary to utilize forensic software tools to perform and analysis of a variety of digital devices. Students will also learn the role of a digital forensic examiner in both the private and public sector. Students will be introduced to fundamental principles of digital forensics investigations.
*Prerequisite: CBY 200*

**CBY 225: Intrusion, Incident Response, and Crisis Management (3 credits)**
This course will provide students with the knowledge and skills required to collect and interpret evidence related to network intrusions such as: network traffic, network devices, servers and operating systems. Specifically, students will learn crisis management skills while collecting and analyzing network traffic and protocols.
*Prerequisite: CSC 210*

**CBY 230: Risk Management (3 credits)**
This course is designed to provide students with ways to identify, manage, respond to and document risk-related events. Specifically, this course will address various stakeholders' perspectives when considering risk. Students will understand concepts and develop a risk management mindset. Finally, students will learn to develop communication and documentation strategies related to risk management.

**CBY 301: Fundamentals of Information Assurance (3 credits)**
This course builds a common cross-disciplinary understanding in the foundations of information assurance. Presents an overview of basic principles and security concepts related to information systems, including workstation security, system security, and communications security. It introduces information security via database technology, discusses legal infrastructure such as DMCA, Telecommunications Act, wire fraud, and other ethical issues. Covers security methods, controls, procedures, economics of cybercrime, criminal procedure, and forensics. It describes the use of cryptography as a tool, software development processes, and protection.

**CBY 310: Cyber Investigations II (3 credits)**
This course prepares students to conduct forensic investigations on Microsoft Windows systems. Students will learn where and how to locate Windows systems artifacts. They will also gain an understanding of the types of evidence associated with a variety of crimes. Students will learn advance concepts such as data carving, live and static filtering, acquisition, and password recovery.

**CBY 315: Secure Software Engineering (3 credits)**
Students in this course will learn why Information Security is critical in our world today. Students will gain an understanding the necessary steps we must take to protect our Personal Identifiable Information (PII) to protecting company suppliers (supply-chain), customers, and overall company assets. Students will also learn why secure software requires implementing secure practices early in the Software Development LifeCycle (SDLC), by adhering to the concepts that enable further understanding of the challenges of insecure and vulnerable software.
*Prerequisite: CSC 101*

**CBY 320: Cyber Strategy (3 credits)**
This advanced course teaches specific skill sets so students will be cyber aware and have a cyber risk mindset across various industries. It provides examples of the evolution of contemporary risk strategies by using case studies from both large and small organizations (e.g., supply chains). By the end of the course, students will be able to communicate various cyber strategies to various stakeholders.

**CBY 330: Mobile Technology Analysis I (3 credits)**
This course provides the knowledge and skills necessary for entry level mobile device examiners to gain a basic understanding of how cellular devices store data, how cellular networks function, collecting evidence and preserving it, methods for radio frequency interruption, troubleshooting connections, verifying results, and the forensic process.

**CBY 335: Data Privacy (3 credits)**
This course identifies legislation, policies and frameworks in the US and the EU related to computer and digital privacy, building upon earlier CBY curriculum. Students will learn concepts of personally identifiable information (PII) across multiple platforms and industries. From a risk management perspective, by the end of the course, students will understand how to protect PII and data privacy.

**CBY 430: Mobile Technology Analysis II (3 credits)**
This course prepares students to perform a forensic examination of mobile technologies by examining the process of collection of artifacts from handsets and SIM cards, extraction of physical data from various device types: like IOS and Android, parsing data, searching, bookmarking, visualization, and incorporation of forensic software, export and reporting.
*Prerequisite: CBY 330*

**CBY 435: Internet Forensics (3 credits)**
This course introduces digital forensic processes, methods and software to recover forensic information from Internet artifacts from a variety of Internet based applications and browsers.
*Prerequisite: CBY 220*

**CBY 440: Cloud Computing (3 credits)**
In this course students are introduced to cloud computing - its history, current practices and systems, and underlying technologies. Students will learn concepts of service delivery and deployment models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This course will also cover new trends in cloud computing, deployment models, principles of cloud architecture, security, privacy and governance.

**CBY 455: Cybersecurity Capstone (3 credits)**
This capstone course is designed to provide an opportunity for the student to synthesize, reflect upon, and analyze the complex and robust field of cybersecurity. This course will highlight the major current issues in the field of cybersecurity.
*Prerequisite: CBY 202, CBY 301, and CSC 210*

**CBY 498: Cybersecurity Internship (3 credits)**
The internship in cybersecurity is a supervised practical learning experience designed to give students the opportunity to explore career interests in fields related to cybersecurity, to acquire valuable on-the-job experience, and to put into practice the knowledge and skills acquired through course work.

**CBY 499: Cybersecurity Internship (6 credits)**
The internship in cybersecurity is a supervised practical learning experience designed to give students the opportunity to explore career interests in fields related to cybersecurity, to acquire valuable on-the-job experience, and to put into practice the knowledge and skills acquired through course work.

**CBY 510: Foundations of Cybersecurity Management (3 credits)**
This course provides an understanding of IT infrastructure and services, their vulnerabilities as well as the size and complexity of security threats faced by enterprises. The Course will focus on the tenets of cybersecurity of confidentiality, integrity, availability and governance. Building on an understanding of these infrastructures, the development of security practices, policies, and awareness and compliance programs, with an introductory look at legal and regulatory issues will be examined in the context of assurance and security. Issues of access and authentication; data confidentiality and integrity; data availability; and networking and routing will also be addressed.

**CBY 515: Foundations of Data Protection (3 credits)**
This course provides students with an understanding of fundamental data protection techniques for protecting data at rest, data in motion, and data in processing. Techniques of data protection such as a basic overview and understanding of cryptology, encryption and other protection schemas and systems which are important for managers to understand will be considered. The course will also examine access controls; availability, authentication, confidentiality, data integrity, and non-repudiation are covered as well as an overview of defenses against DDOS and other data attacks. Security by diversity and security in depth will be presented as fundamental requirements. Issues of access and authentication; data confidentiality and integrity; data availability; and networking and routing will also be addressed.

**CBY 620: Compliance and Legal Issue (3 credits)**
This course examines legal, privacy and compliance environments facing US based organizations. Students will build an understanding of the complexities of these compliance and legal obligations starting with a general foundation of laws and industry standards that apply across most organizations. The course will review the legal aspects of customer information safeguards. Examination of industry verticals will expand the student's knowledge of particular federal and state regulatory and industry-based obligations. This course will also introduce the relevant laws and regulations with regard to law enforcement and civil investigation of digital crimes.

**CBY 625: Financing, Cost Control, and Proj. Mgmt. of Cybersecurity Orgs. (3 credits)**
This course explores Information Assurance Management through finance and cost controls. The course will look at the strategic costs, financing and project management of important organizational IT functions. The course will also explore the aspects, methods, and alternatives in financing and cost control in information assurance management and compares/utilizes them with respect to non-IT-related expenses and costs. This seminar will also discuss and develop how to determine the costs and management of projects and compliance. The course also explores alternatives in building support and consensus for projects and activities and focuses heavily on adding value to the organization. Moreover, the course explores methods to build support and consensus for projects and activities while adding value to the organization. Financing and cost are explored both in terms of measuring business impact, problem solving and project management.

**CBY 630: Emerging Cyber Threats (3 credits)**
This course examines the current topics of cybersecurity attacks and defenses from a global perspective. Security incidents will be analyzed and technologies and processes studied to better understand how to prevent or minimize a similar threat in the future. The course will be a mixture of traditional concerns around virus protection and spam prevention with new threats introduced by technology such as mobile devices and cloud computing.

**CBY 635: Human and Organizational Aspects of Cybersecurity (3 credits)**
This course investigates the relationships between human and organizational behavior and cybersecurity. Emphasis is on the human and OB elements of cyber-crimes. Topics will include ethics, psychology, sociology, hacker and organizational culture. Motivations for cybercrime and breaches of cybersecurity will be investigated. This course will consider social psychology and positive psychology and how behaviors influence the effectiveness of security practices. The courses will talk about best employment and risk management practices and policies to support information assurance and security including social network and email policies. The focus is on the ways that business objectives, user attitudes and user activities significantly influence both the development of an information assurance program and successful implementation of such programs.

**CBY 640: Information Assurance Management and Analytics (3 credits)**
This seminar is arranged beginning with examining and exploring Information Assurance Management and Analytics from a strategy perspective and gradually narrowing down to the tactical level, including the management of projects and compliance; leadership and policy development; relationship building in an organization; and organizational education. The course will also review customer information safeguards. The curriculum explores the aspects, methods, and alternatives in information assurance management and compares/utilizes them with respect to non-IT-related management approaches and styles. Additionally, it explores alternatives in building support and consensus for projects and activities and focuses heavily on adding value to the organization. Developing an information assurance management plan is examined and is used to help identify techniques of improving the information assurance awareness. Analytics are explored both in terms of measuring business impact, and problem solving and project management techniques and alternatives are included.

**CBY 645: Cyber Criminal and Civil Investigations (3 credits)**
This course provides an analysis of the use of industry tools, technologies, and practices involved in gathering, protecting and analyzing digital evidence. The class uses industry tools to perform forensic analysis and examines how various operating systems store data on storage media - hard disk drives and other digital media. The course will highlight how computers are used in crimes and how this can be linked to criminal motivations to focus a digital investigation. Students will gain an in-depth study of the theories and practices for the prevention of cyber-attacks. Countermeasures discussed include training, encryption, virtual private networks, policies, practices, access controls, secure systems development, software assurance arguments, verification and validation, firewall architectures, anti-virus, patching practices, personnel security practices, and physical security practices. Business continuity plans and disaster recovery plans are also discussed. Strategies for large-scale prevention are also discussed, such as critical infrastructure protection, international collaboration and law enforcement. Emphasis is on methods to identify system vulnerabilities and threats and prevent attacks.
*Prerequisite: CBY 610 and CBY 615*

**CBY 650: Strategic Cybersecurity Crisis Management (3 credits)**
This course focuses on operational cybersecurity management issues in business continuity planning, disaster recovery, identity management, change management, metrics, accreditation, certification, and validation. The course examines in detail effective risk assessment programs, disaster recovery planning, how to interpret the sources and levels of risk, how to apply appropriate defensive systems employing security in depth and diversity concepts, and back-up and recovery procedures. Students are required to examine cybersecurity at a program and architectural level regarding issues such as risk management, audit, privacy, Information Security Management System (ISMS), and identify how management will respond to a disaster within an organizational context. Students will also be able to limit and mitigate loss, teach security awareness, metrics and develop educational strategies, and then present a plan to the executive board for approval.

**CBY 655: Digital Forensics (3 credits)**
In this course, the student will accomplish in-depth studies of the theory and practice of digital investigations in criminal and civil cases on a local, state, national and global basis. Topics include cyber terrorism, cybercrime and cyber warfare. Discussions will also include identification, collection, acquisition, authentication, preservation, examination, analysis and presentation of evidence for prosecution purposes. In addition students will discuss the elements of management and leadership required in the field of investigation.

**CBY 657: Advanced Digital Forensics (3 credits)**
In this course students will explore advanced aspects of working a variety of digital forensic case. Students will develop a methodology for learning as much about the targeted subject and the case as possible during the initial phase of your preliminary or full analysis. Students will have the opportunity to utilize both proprietary and open source tools throughout this course. An analytic approach will be used to provide students with the knowledge and skills to analyze evidence from a different perspective and we will see why it is important to not limit your analysis to just one tool.

**CBY 658: Cloud Forensics (3 credits)**
In this course students will explore advanced aspects of working a variety of digital forensic case. Students will develop a methodology for learning as much about the targeted subject and the case as possible during the initial phase of your preliminary or full analysis. Students will have the opportunity to utilize both proprietary and open source tools throughout this course. An analytic approach will be used to provide students with the knowledge and skills to analyze evidence from a different perspective and we will see why it is important to not limit your analysis to just one tool.

**CBY 659: Mobile Device Analysis (3 credits)**
This course will provide students the ability to identify and analyze the various data types and structures found on mobile devices and how they are stored. Students will learn both manual and automated parsing and analysis of data so that they will be able to combine data recovered from both automated tools and manually recovered data. This comprehensive approach will provide students the advanced skills necessary to generate more relevant and complete investigative reports.

**CBY 660: Cyber Policy (3 credits)**
This course will examine the role of various official and non-official agencies, domestic, international, governmental and non-governmental in setting cybersecurity policy. This is a dynamic examination of the issues surrounding cyber policy issues and includes: intellectual property and civil liberties, privacy concerns and national security issues. Given the fluidity of the field an examination of current laws, policies and standards is undertaken.

**CBY 661: Intrusion Detection and Incident Response Investigations (3 credits)**
This course will provide students with the knowledge and skills required to collect and interpret evidentiary evidence related to network intrusions such as: network traffic, network devices, servers and operating systems. Specifically students will have the opportunity to collect and analyze network traffic, including TCP/IP and higher level protocols.

**CBY 662: Expert Witness and Reporting (3 credits)**
This course will acquaint the student with the qualifications and duties of an expert witness. Through the use of technology, case studies and specific guidelines, students will be prepared to serve as an expert witness in a variety of legal settings relating to the presentation of digital forensic evidence.

**CBY 663: Data Structures and Python (3 credits)**
This course prepares students with the knowledge and skills necessary to utilize open source and commercial software to create Python scripts and programs. Students will demonstrate knowledge of fundamental computer programming principles such as variables, operands, conditional statements, functions, looping, strings, lists, dictionaries and tuples. These basic concepts and related terminology will be reinforced through weekly hands-on assignments, discussions and quizzes. Students will broaden their knowledge and understanding of what a computer programmer does and the types of skills needed in both the private and public sectors. Students will be required to demonstrate their proficiency in programming and a familiarity with the Python programming language through online reference material, discussions, applied practical exercises, weekly help sessions and quizzes. Learning by working in a team environment is emphasized.

**CBY 670: Capstone I: Cyber Thesis (3 credits)**
A study of and an exercise in developing, leading, and implementing effective enterprise level cybersecurity programs in a real-life setting. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries are discussed. Topics include enterprise architecture, risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning. A project paper is the major focus of the learning experience as it will reflect integration and synthesis of the entire cybersecurity curriculum. As part of this project the student will be able to define a program for one or a variety of users and/or develop sophisticated implementation policies for companies, agencies or governments. Must be taken as the last course in the program. Student must take either CBY 670 or CBY 675, not both.

**CBY 675: Capstone II: Cyber Plan (3 credits)**
This course presents a study of and an exercise in developing, leading, and implementing effective enterprise level cybersecurity programs in a real life setting. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries are discussed. Topics include enterprise architecture, risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning. A project plan for an existing organization will be developed and it will reflect integration and synthesis of the entire cybersecurity curriculum. The student will be able to define a plan for one or a variety of users and/or develop sophisticated implementation policies for companies, agencies or governments. Prior to beginning the plan, the student should select and meet with the company to receive permission to do this study. The information, if proprietary, may require certain confidentiality agreements and privacy restrictions between the professor, the company and you. Must be taken as the last course in the program. Students must take either CBY 670 or CBY 675, not both.

**CBY 698: Cybersecurity Internship (3 credits)**

**CBY 699: Cybersecurity Internship (6 credits)**