WESTMINSTER COLLEGE

CYBERSECURITY MINOR

Professor: L. Webster
Instructor: C. Cox

Contact: Dr. Linda Webster
Email: linda.webster@wcmo.edu

A minor in Cybersecurity will enhance the skills of students in any discipline by preparing them to be knowledgeable consumers of digital resources and aware of the associated risks. The issue of Cybersecurity is not unique to any one type of organization. Businesses, nonprofit organizations, and governments all face security issues related to computing technology. Social organizations, clubs, and political groups face similar issues. Students who complete a minor in Cybersecurity will be prepared to identify cyber risks to an organization and work with information technology security specialists to protect the digital assets of that organization. All disciplines rely on digital communication, files, and other assets; thus, this program will be relevant to a student in any discipline who is interested in protecting digital assets.

You can find the course descriptions for all courses required for this minor by clicking on the following links:

- Cyber Security Course Descriptions
- Security Studies Course Descriptions

ACADEMIC REQUIREMENTS SUMMARY SHEET ACADEMIC YEAR 2022-2023

____
Student's Last Name First Name Middle Initial

____
Advisor Date Minor Declared

Course #	Title of Course	Hours Required	Semester Completed	Grade
Required Courses:				
CBR 110	Introduction to Cybersecurity	3		
CBR 220	Information Security	3		
CSA 250	IT Infrastructure	3		
CBR 360	Cyber Law and Ethics	3		
CBR 415	Information Security Policy	3		
CBR 470	Cybersecurity Capstone	1		
TBD	3-hour elective course pre-approved by the CBR minor advisor selected from a discipline other than CBR and related to the field of cybersecurity and the capstone project.	3		
	TOTAL HOURS FOR MINOR	19		

If any substitutions or waivers of requirements are allowed, please list below and initial.

____

____

CBR – Cybersecurity

CBR 110 Introduction to Cybersecurity (3 hrs.) This course will introduce the field of cybersecurity and explore cybersecurity issues from national, international, transnational, institutional, and personal perspectives. We will utilize critical thinking to examine issues facing individuals and society, regardless of culture, such as terrorism, identity theft, and how individuals can be effective and safe users of technology. Readings and discussions from current literature will be included. Prerequisites: None. Offered every fall.

CBR 220 Information Security (3 hrs.) This course will introduce practices and policies for deterring, detecting, and responding to cyber attacks on an organization. Topics include computer forensics, software security, information assurance, intrusion detection, network security, cloud computing, business continuity, identity theft, and threat identification. Risks and vulnerabilities will be explored in the areas of computing hardware and devices, users, digital network and communications, and data. Prerequisites: None. Offered every spring.

CBR 331 Information Storage Management (3 hrs.) This course provides a comprehensive introduction to storage technology which will enable the student majoring in any discipline to make more informed information storage decisions in the increasingly complex environment of a modern storage infrastructure within any organization. All organizations and academic disciplines are increasingly dependent on data and information residing on some form of network-based storage and dependent on its security, reliability, performance, and availability 24/7. The course focus is on storage architectures, features, and benefits of Intelligent Storage Systems including networked storage technologies; long-term archiving solutions; and the increasingly critical areas of information security, the emerging field of storage virtualization technologies, and information availability and business continuity. This course is appropriate for students from any discipline who desire to know more about managing the risks and features of information storage. Prerequisite: CBR 210 Cybersecurity for Society. Offered in the spring of every odd year.

CBR 332 Digital Network Security (3 hrs.) This course provides an overview of the area of digital computer networks and communication, including concepts and designs. Topics to be covered include networking models, and how data signals are transmitted and received. It explores the tradeoff between risk and access, and presents the security vulnerabilities that occur within a networked environment. Network security and defenses at the hardware, software, and policy levels will be identified. Hands-on lab activities will be used to reinforce the topics covered in the course. Prerequisites: CBR 210 Cybersecurity for Society OR CBR 220 Information Security. Offered in the fall of every even year.

CBR 340 Digital Forensics (3 hrs.) This course focuses on the tools and processes used by cybersecurity professionals to monitor, detect, and respond to cyber threats to an organization and other various types of computer crimes. Emphasis is placed on the acquisition and preservation of digital artifacts and evidence, data recovery, and information assurance. Hands-on lab activities will provide the students with opportunity to employ some of the current tools used for these purposes. Prerequisite: CBR 220 Information Security. Offered every spring semester.

CBR 360 Cyber Law and Ethics (3 hrs.) Students in this class will explore legal and ethical issues related to the Internet, digital data, and the use of digital assets and how these constantly emerging issues effect society. Some of the topics explored in this class includes individual privacy, intellectual property, cyberbullying, censorship, fake news, discipline-specific compliance and regulations, and other current legal and ethical issues. Since the Internet and digital communication can easily cross the globe, an organization's digital assets may be controlled by the laws and ethics of another country. Students will learn how to develop appropriate information security policies and responses based on both legal and ethical considerations. Prerequisites: CBR 110 or CBR 220. Offered every spring.

CBR 415 Information Security Policy (3 hrs.) In our data driven, decision-oriented world in which we live, information is a critical and valuable asset of an organization. From real time data mining to global availability, the information of any organization today must be immediate, constant, and reliable. This course will use risk assessments of threats to business continuity/information availability (BC/IA) to plan for BC/IA needs, and describe the critical role that all members of an organization play in the IT BC/IA analysis and planning process. Topics will include data backup, replication, and archival; information security; cloud computing; and disaster recovery. As a final project, students will either develop a BC/IA plan for an actual organization or research a course topic in more depth. While this course is presented from a cybersecurity perspective, it is appropriate for students from any discipline who desire to know more about the dependencies between information, organization, and technology. Prerequisites: CBR 210 Cybersecurity for Society OR CBR 220 Information Security. Offered every spring semester.

CBR 470 Cybersecurity Capstone (1 hr.) This course provides students the opportunity to consolidate the coursework in the study of cybersecurity minor into a single capstone experience, although a minor in CBR is not a prerequisite. Working with the CBR minor advisor, students will select an appropriate project based on their interests and career goals within the field of cybersecurity. They may choose to emphasize a specific aspect of Cybersecurity, such as technical implementation, data analysis and decision-making, organizational policies, or national and international political implications. These research project will require the student to identify a topic, formulate a research plan, develop a project plan and timeline, conduct research, and prepare a culminating work. This work may include a research paper, policy recommendation, information assurance and business continuity plan for an organization, data analysis project, or procedures for monitoring and detecting and organization's digital assets. Prerequisites: CBR 110 or CBR 220; AND a non-CBR course related to cybersecurity pre-approved by the CBR Minor advisor. Offered as an independent course as needed.

SEC – Security Studies

SEC 201 Introduction to Security Studies (3 hrs.) This course will provide the foundations for the Security Studies minor and major, and will serve to introduce many issues in the modern search for security. By the end of the course, you should have a basic understanding of the major theories of security; current issues, conceptions threats to security; institutions related to security; and identify future threats that may loom on our horizon. Additionally, there will be several guest speakers in class who will discuss particular issues in more detail.

SEC 205 Intro to Homeland Security (3 hrs.) The principal objective of this course is to provide a comprehensive introduction to US homeland security, with a focus on the post-September 11, 2001 era. We will examine agency missions, laws, and regulations that govern America's efforts to protect the homeland. Through an examination of complex threats and threat environments, students will gain insight into contemporary issues relevant to the homeland security enterprise

SEC 312 Terrorism (3 hrs.) The major objective of this course is to increase your knowledge about terrorism: what it is, why it occurs, why targets are selected, and how to prevent it. Prerequisites: SEC 201.

SEC 325 Issues in Homeland Security (3 hrs.) The purpose of this class is to provide an understanding of the issues and policy spaces that comprise homeland security. The policy space is wide and oft-changing; as such, this course is designed to introduce the students to the critical policy spaces, and allow the student to explore these with some depth. Prerequisites: POL 211; POL 301; any Security Studies course (SEC designation); OR permission of the instructor.

SEC 328 National Security Agencies (3 hrs.) To understand the politics and processes of national security we must have an understanding of the national security labyrinth at the national level. The purpose of this course is to ensure the students' knowledge about the institutional design, oversight mechanisms and shortcomings, missions, and relationship of the varied institutions of the national security bureaucracy. Prerequisites: POL 211, SEC 201, or permission of the instructor.

SEC 334 Intelligence at Home and Abroad (3 hrs.) Nations survive and prosper on the basis of their ability to effectively gather, evaluate, and utilize information about threats. In this course, students will examine the history, context, purpose, methods, processes, and challenges of intelligence gathering at home and abroad. Prerequisites: SEC 201, POL 212, or permission of the instructor.

SEC 335 Politics and Security of Developing Nations (3 hrs.) In this course, students will undertake a comparative investigation of the political dynamics of the developing world. Looking across Latin America, Asia, and Africa, students will identify and contrast patterns of political behavior across regions and analyze models of economic development, governance, and security challenges that occur in the developing world. By taking a policy-making perspective, students will assess problems and analyze solutions to current issues in developing nations. Prerequisites: POL 112, 212, SEC 201 or permission of the instructor.

SEC 337 Human Rights and Security (3 hrs.) This course examines the evolution of the international system of human rights. It will consider fundamental legal, moral, and political debates related to human rights and look for avenues to make progress in human rights protection. It will also examine the relationship between human rights and human security and the challenges associated with the provision of human security in the 21st century, with special attention paid to human trafficking and economic development. Prerequisites: POL 112, 212, SEC 201, GTS 201, or permission of the instructor.

SEC 346 Chinese Politics and Influence (3 hrs.) An examination of how China's emergence as an economic, diplomatic, and military heavyweight is shifting the global balance of power, shaping the responses of governments and intergovernmental organizations, and posing fundamental questions about the nature of world order itself. Prerequisites: GTS 201, SEC 201, POL 212, or permission of the instructor.

SEC 364 Stereotyping, Prejudice, and Group Conflict (3 hrs.) This course uses experimental social psychology as the foundation to explore the affective, behavioral, and cognitive processes associated with group interaction and conflict. Utilizing an interdisciplinary perspective, it will integrate psychological, sociological, political, historical, and security-related approaches to understanding stereotypes, prejudice, and discrimination on a local and global scale. Offered occasionally. Prerequisite: PSY 113.

SEC 420 Security Studies Thesis (3 hrs.) Students will learn research methods and utilize them to write a thesis paper. The expectation is that these papers will be written at a level acceptable for off-campus conference. Prerequisites: junior or senior status; declared Security Studies major; 18 or more hours toward major completion. Students will learn research methods and utilize them to write a thesis paper. The expectation is that these papers will be written at a level acceptable for off-campus conference. Prerequisites: junior or senior status; declared Security Studies major; 18 or more hours toward major completion.