Bachelor of Science in Cybersecurity (BCS)

Our unique approach to teaching combines the theoretical with the practical, as faculty bring extensive real-world technology experience to the classroom. Classroom instruction is often augmented with outside technology speakers and information technology facility visits. In many courses, student projects involve solving technology problems and providing information technology services to actual real-world organizations. Additionally, all students complete a series of cybersecurity internships prior to graduation. These internships can lead to permanent employment opportunities.

Requirements for the BSM Degree

√	Degree Component
	Completion of the Bachelor General Education Core (54 credits) **CS 101S and MT 122S** are required in the Gen-Ed
	Completion of the General Education Competencies
	Completion of the Cybersecurity Major Courses (60 credits)
	Completion of the bachelor of science electives (12 credits) **BS 206S** is required as one of the BS elective courses
	Completion of 126 credit hours (two terms and 32 credit hours must be completed at Montreat College)

If students take a full-time load each term, they could complete this program in four years.

BCS Prerequisites

- CS 204S Fundamentals of Information Systems requires students to first meet computer competency. This prerequisite must be met by successful completion of one of the following (minimum grade of *C*) within the last ten (10) years:
    - **CS 101S** Computer Applications and Concepts
    - Equivalent introductory computer course from a regionally accredited college or university (official transcript showing proof must be submitted to the Office of Records and Registration)

  In addition to fulfilling the pre-requisite requirement, the above course will earn three hours of general education credit.

12 Bachelor of Science Hours

Students pursuing a Bachelor of Science degree must complete an additional 12 hours beyond the General Education Core and major requirements in mathematics, science, business, computer, or other designated coursework as listed in the degree requirements for each program of study. This coursework may not be applied to the General Education Core, the major, r any major concentration requirements. For the Cybersecurity major, students must take **BS 206S** Principals of Accounting which will count toward this requirement.

Bachelor of Science in Cybersecurity Courses

CS 204S	Fundamentals of Information Systems	3
CS 207S	Prin of Op Systems and Comp. Hardware	3
CS 215S	Intro to Comp. Networking	3
CS 335S	Computer & Systems Security	3
CS 345S	Principles Of Cybersecurity	3
CS 350S	Management of Cybersecurity	3
BS 350S	Admin. Theory & Org. Behavior (5 weeks)	3
CS 221S	Intro to Secure Programming Logic	3
IS 310S	Pre-Internship or equivalent (5 weeks)	3
CS 290S	Principles of Cyber Defense	3
CS 242S	Cybersecurity Internship I (45 hours: 16 weeks)	1
CS 310S	Database Programming	3
CS 365S	The 3 C's: Cybercrime, Cyber Law & Cyber Ethics	3
CS 370S	Network Defense and Countermeasures	3
CS 342S	Cybersecurity Internship II (45 hours: 16 weeks)	1
CS 375S	Linux Operating Systems and Security	3
CS 428S	Penetration Testing	3
CS 438S	Network Forensics	3
CS 442S	Cybersecurity Internship III (45 clock hours: 16 weeks)	1
CS 490S	Advanced Cyber Defense	3
CS 448S	Incident Response and Contingency Planning	3
CS 492S	Adv Cyber Internship & Senior Project (90 clock hours: 16 wks)	3
TOTAL		**60**

CS 101S Computer Applications and Concepts

An introduction to computer hardware and software, with an emphasis on basic applications and concepts. Basic competence with word processing, online learning, and Internet navigation and communication will be acquired. The course includes an introduction to spreadsheets and presentation software. *Computer usage competency.* (3 credits, 5 weeks)

CS 203S Information Systems Technology for Managers

This course provides a thorough overview of information systems technology for management. Through lecture, case study, Internet exploration and hands-on applications, students examine a wide variety of critical uses of information technology by management. *Prerequisite: completed computer usage competency* (3 credits, 5 weeks)

CS 204S Fundamentals of Information Systems

Providing an introduction to systems and development concepts, information technology, and application software, this course explains how information is used in organizations and how information technology enables improvement in quality, timeliness, and competitive advantage in organizations. Topics include systems concepts, system components and relationships, cost/value and quality of information, competitive advantage and information, specification, design and reengineering of information systems, application versus system software, and package software solutions. *Prerequisite: CS 102S or equivalent competency* (8 weeks, 3 credits)

CS 207S Principles of Operating Systems and Computer Hardware

An in-depth study of operating systems and computer hardware covering the domains of the A+ Certification. Focus is on identification, installation, configuration, and troubleshooting of field replaceable components. Topics include microprocessors, memory, BIOS and CMOS, expansion bus, motherboards, power supplies, floppy drives, hard drives, removable media, video, audio, portable PCs, printers, networks, the Internet, computer security, and Windows operating systems. *Prerequisite: CS 204S* (3 credits, 8 weeks)

CS 208P Microsoft Excel Introductory

This course uses excel to create basic spreadsheet applications containing formulas with absolute and relative cell addressing, built-in functions, charts, and drawing objects. This course covers the following Excel skills: creating and editing worksheets containing data and formulas, managing workbooks and files, modifying worksheets through copy and paste, drag and drop, Auto fill, and inserting and deleting rows and columns, and formatting and printing worksheets to enhance worksheet appearance and customize print output. The course is conducted using a case-based, problem solving approach emphasizing the What, Why, and How of the above Excel application skills. *Prerequisite: completed computer usage competency.* (3 credits, 5 weeks)

CS 209P Microsoft Excel Intermediate

This course covers the following skills: *using date & time, financial, and logical functions in decision-making applications; *organizing, manipulating and consolidating data in large worksheets and multiple worksheet applications; *creating, sorting, and filtering worksheet lists; *analyzing decision alternatives using Pivot Tables, data tables, goal seeking, solver and scenario manager; *using lookup and reference functions; *importing and exporting data; *developing workbook applications including workbook sharing, conditional formatting, data validation and macro automation. *Prerequisite: CS 208P or equivalent*. (3 credits, 5 weeks)

CS 215S Introduction to Computer Networking

An in-depth study of computer networking theories and concepts covering the domains of the Network+ Certification. Focus is on the configuration, maintenance, and troubleshooting of network devices using appropriate network tools and understanding of the features and purpose of network technologies. *Prerequisite: CS 207S* (3 credits, 8 weeks)

CS 221S Introduction to Secure Programming Logic

This is an introductory course in structured programming logic. Students will learn to analyze problems; define data using simple data types and arrays; and create algorithmic solutions using basic control structures (sequence, selections, and loops) and functions. Students learn to systematically break down a problem into manageable parts; plan and design logical solutions; and write effective, structured, and well-documented instructions. Emphasis will be on problem-solving approaches (algorithms) and the fundamental concepts and programming techniques common to modern computer languages including variable assignment, expressions, input/output statements, loops, if-then-else and case constructs, functions, arrays, etc. The concepts learned in this course are applicable to multiple modern programming languages. *Prerequisite: CS 204S or permission of professor* (3 credits, 8 weeks)

CS 242S Cybersecrutiy Internship I

This initial supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with coursework completed. Students will be required to document a minimum of 45 clock hours of internship engagement and reflection in the course. A total sequence of three internship courses is required in the program of study (CS 242S, CS 342S, CS 442S are all required for degree).
(16 weeks, 1 credit)

CS 290S Priciples of Cyber Defense

A practical application of the theories and practices for prevention of cyber-attacks. Students will discuss and practice countermeasures including encryption, policy-making, monitoring of access controls, development of secure systems, as well as the review of verification and validation measures. Primary focus will be on Windows systems software. (8 weeks, 3 credits)

CS 310S Database Programming

A course introducing the student to the logic, design, implementation, and accessing of organizational databases as contrasted to older conventional data file techniques introduced in COBOL programming. Particular emphasis is placed on relational database management that focuses on the logical nature of databases. Popular microcomputer-based database programs will be utilized. *Prerequisite: CS 221S or permission of professor* (8 weeks, 3 credits)

CS 335S Computer and Systems Security

An in-depth study of computer and systems security covering the domains of the Security+ Certification. Focus is on the knowledge and skills required to identify ethical challenges and risk, and to participate in risk mitigation activities, provide infrastructure, application, operational and information security, apply security controls to maintain confidentiality, integrity and availability, identify appropriate technologies and products, and operate with an awareness of applicable policies, laws and regulations. Pre-requisite: CS 215S. (8 weeks, 3 credits)

CS 342S Cybersecurity Internship II

This second supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with coursework completed. Students will be required to document a minimum of 45 clock hours of internship engagement and reflection in the course. A total sequence of three internship courses is required in the program of study (CS 242S, CS 342S, CS 442S are required). (16 weeks, 1 credit)

CS 345S Principles of Cybersecurity

Examination of current standards of due care and best business practices in Cybersecurity. Includes examination of security technologies, methodologies and practices. Focus is on the evaluation and selection of optimal security posture. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning and security policy formulation and implementation. **Prerequisite: CS 335S** (8 weeks, 3 credits)

CS 350S Management of Cybersecruity

Detailed examinations of a systems-wide, ethically framed perspective of Cybersecurity, beginning with a strategic planning process for security. Includes an examination of the policies, procedures and staffing functions necessary to organize and administrate ongoing security functions in the organization. Topics include ethical security practices, security architecture and models, continuity planning and disaster recovery planning. *Prerequisite: CS 345S* (8 weeks, 3 credits)

CS 365S The 3 C's: Cybercrime, Cyber Law and Cyber Ethics

A study of the impact of cybercrimes affecting various entities and organizations engaged in cyberspace transactions and activities including the government, military, financial institutions, retailers and private citizens. The course covers broad areas of law pertaining to cyberspace, including Intellectual Property (Copyright, Patent, Trademark, and Trade Secret), Contract, and the U.S. Constitution. The study of Cyberethics addresses a definition of ethics, provides a framework for making ethical decisions undergirded by a biblical worldview, and analyzes in detail several areas of ethical issues that computer professionals are likely to encounter in cyberspace and in business. Real-world current events topics and case studies are deployed and discussed each week. (8 weeks, 3 credits)

CS 370S Network Defense and Countermeasures

Detailed examination of the tools and technologies used in the technical securing of information assets. This course is designed to provide in-depth information on the software and hardware components of Cybersecurity. Topic covered include: firewall configurations, hardening Linux and Windows servers, Web and distributed systems security, and specific implementation of security models and architectures. *Prerequisite: CS 345S* (8 weeks, 3 credits)

CS 375S Linux Operating Systems and Security

An in-depth study of Linux operating system covering the domains of the Linux+ Certification. Focus is on implementing GNU and UNIX commands from the command line, installing and configuring Linux, and maintaining securing the Linux system. *Prerequisite: CS 215S* (8 weeks, 3 credits)

CS 428S Penetration Testing

A detailed examination of real world cybersecurity knowledge, enabling recognition of vulnerabilities, exploitation of system weaknesses, and safeguards against threats, all through the application of an ethical framework and biblical worldview. Students will learn the art of penetration testing through hands-on exercises and a final project. Students who complete this course will be equipped with the knowledge necessary to analyze and evaluate systems security. *Prerequisite: CS 370S or permission of professor* (8 weeks, 3 credits)

CS 438S Network Forensics

In this course, students will learn to identify network security events, incidents, intrusions and sources of digital evidence in a lab environment while applying an ethical framework. The students will develop a comprehensive understanding of network forensic analysis principles including identifying and categorizing incidents, responding to incidents, log analysis, network traffic analysis, and using various tools to integrate network forensic technologies. Student will demonstrate the ability to accurately document network forensic processes and analysis. *May be taken concurrently with CS 428S or permission of professor* (8 weeks, 3 credits)

CS 442S Cybersecurity Internship III

This third supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with coursework completed. Students will be required to document a minimum of 45 clock hours of internship engagement and reflection in the course. A total sequence of three internship courses is required in the program of study (CS 242S, CS 342S, CS 442S are required). (16 weeks, 1 credit)

CS 448S Incident Response and Contingency Planning

An examination of the detailed aspects of incident response and contingency planning consisting of incident response planning, disaster recovery planning, and business continuity planning. Developing and executing plans to deal with incidents in the organization is a critical function in information security. This course focuses on the planning processes for all three areas of contingency planning – incident response, disaster recovery and business continuity, as well as the execution of response to human and non-human incidents in compliance with these policies. Case studies and strategies for implementation of corporate breach prevention, critical infrastructure protection, and intersection of law enforcement are discussed. *Course should be taken concurrently with CS 492S. Prerequisite: CS 370S or permission of professor* (8 weeks, 3 credits)

CS 490S Advanced Cyber Defense

This capstone course discusses the hardware/software tools and techniques associated with the protection of computer systems and networks, including Linux software. Students learn how to protect network resources in live in-course simulations. Course topics include policy and practice associated with the protection of communication resources, intrusion detection systems, firewalls, and use of anti-virus, patching practices, as well as personnel and physical security practices. *Prerequisite: CS 370S or permission of professor* (8 weeks, 3 credits)

CS 492S Advanced Cybersecurity Internship & Senior Project

This advanced supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with coursework completed. Students will be required to document a minimum of 90 clock hours of internship engagement and to produce a comprehensive cybersecurity project reflective of the completed program of study. Potential senior projects include business continuity plans and disaster recovery plans. *Course should be taken concurrently with CS 448S. Prerequisite: CS 442S* (16 weeks, 3 credits)