Cybersecurity Major

Bachelor of Science in Cybersecurity Degree Mission Statement

The mission of the Business and Cybersecurity Department is to equip students with knowledge necessary for them to serve in today’s competitive business environment and to cultivate in all students, at all levels, (undergraduate and graduate) a data-driven approach and ethical spirit in their approaches to business decision making.

Cybersecurity Program Goals

1. Ability to integrate Christian worldview and ethics in the work environment.
2. Knowledge and experience in information systems technology on business functional areas.
3. Knowledge and experience in Cybersecurity to support organizational mission and goals.
4. Critical thinking, analytical, and problem-solving skills.
5. Effective communications and interpersonal and team skills.

Why Study Cybersecurity at Montreat College?

The program builds upon Montreat College’s strong liberal arts core with extensive training and preparation in information technology, cybersecurity, business administration, and quantitative analysis, preparing students for entry-level professional positions in a variety of technology specializations. Our unique approach to teaching combines the theoretical with the practical, as faculty bring extensive real-world technology experience to the classroom. Small classes provide personal attention and one-on-one interaction with professors. 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 cybersecurity internship prior to graduation. These internships can lead to permanent employment opportunities.
After Graduation

The Cybersecurity degree program prepares graduates for a variety of careers in consulting, financial and banking institutions, health care, services and manufacturing industries, government, and not-for-profit organizations. A graduate of the major may look forward to a Cybersecurity career to support information technology fields such as incident response and business continuity analysis, information systems analysis, programming, database administration, web development, network engineering, systems administration, security analysis, vulnerability assessment, penetration testing or enterprise consulting. According to the Bureau of Labor Statistics, these fields are expected to be among the fastest growing occupations through 2020. Employment of cybersecurity professionals are expected to grow much faster than the average for all occupations as organizations continue to adopt and integrate increasingly sophisticated cybersecurity technologies. Average annual salaries in these fields are well above those in many other professional occupations. Further, many information technology occupations offer broad opportunities to influence others for Christ.

Requirements for a Major in Cybersecurity

- Completion of the General Education Core (56 Credits)  
  MT 114 is required in the Gen-Ed
- Completion of the General Education Competencies
- Completion of the Cybersecurity Major Core (64 credits)
- Completion of the Cybersecurity Major Electives (6 credits)
- Completion of 33 credits at the 300-level or above
- Completion of 126 credit hours with a minimum GPA of 2.0 (two terms and 32 hours must be completed at Montreat college)
Cybersecurity Major Core (64 credits)

- BS 101 Introduction to Business (3)
- BS 201 Principles of Accounting I (3)
- IS 310 Pre-Internship (1)
- CS 204 Fundamentals of Information Systems (3)
- CS 207 Principles of O.S. & Computer Hardware (3)
- CS 215 Introduction to Computer Networking (3)
- CS 221 Introduction to Secure Programming Logic (3)
- CS 289 Cyber Defense I (2)
- CS 310 Database Programming (3)
- CS 335 Computer and Systems Security (3)
- CS 341 Internship I (3)
- CS 345 Principles of Cybersecurity (3)
- CS 350 Management of Cybersecurity (3)
- CS 365 The 3 C’s: Cybercrime, Cyber Law & Cyber Ethics (3)
- CS 370 Network Defense and Countermeasures (3)
- CS 375 Linux Operating Systems and Security (3)
- CS 389 Cyber Defense II (2)
- CS 428 Penetration Testing (3)
- CS 438 Network Forensics (3)
- CS 441 Internship II (3)
- CS 448 Incident Response and Contingency Planning (3)
- CS 489 Cyber Defense III (3)
- MT 121 College Algebra (3) or higher

Required Major Electives (choose 6 hours)

- CS 287 Cyber Competition I (2)
- CS 380 Certification Study and Preparation (3)
- CS 387 Cyber Competition II (2)
- CS 475 Cybersecurity Programs and Strategies (3)
- CS 480 Special Topics (3)
- CS 487 Cyber Competition III (2)
## Four Year Plan: Bachelor of Science in Cybersecurity

### Freshman Year

<table>
<thead>
<tr>
<th>Fall Semester</th>
<th>Spring Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS 102 Foundations of Faith and Learning</td>
<td>BB 102 Survey of New Testament</td>
</tr>
<tr>
<td>BB 101 Survey of Old Testament</td>
<td>EN 102 English Composition II</td>
</tr>
<tr>
<td>EN 101 English Composition I</td>
<td>CS 204 Fund. Of Information Systems</td>
</tr>
<tr>
<td>Gen-Ed Natural Science</td>
<td>Gen-Ed Natural Science</td>
</tr>
<tr>
<td>PE activity course</td>
<td></td>
</tr>
<tr>
<td><strong>16</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>

### Sophomore Year

<table>
<thead>
<tr>
<th>Fall Semester</th>
<th>Spring Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>HS 101 History of World Civilization I</td>
<td>HS 102 History of World Civilization II</td>
</tr>
<tr>
<td>CS 215 Intro to Computer Networking</td>
<td>MT 114 Elementary Probability and Statistics</td>
</tr>
<tr>
<td>CS 221 Intro to Secure Programming Logic</td>
<td>CS 335 Computer and Systems Security</td>
</tr>
<tr>
<td>Gen-Ed Literature</td>
<td>CS 288 Cyber Defense I</td>
</tr>
<tr>
<td>MT 121 College Algebra</td>
<td>IS 310 Pre-Internship</td>
</tr>
<tr>
<td>PE activity course</td>
<td>Gen-Ed Oral Competency</td>
</tr>
<tr>
<td><strong>16</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>

### Sophomore Summer

<table>
<thead>
<tr>
<th>Course</th>
<th>Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 341 Internship I</td>
<td>Fall</td>
</tr>
</tbody>
</table>

### Junior Year

<table>
<thead>
<tr>
<th>Fall Semester</th>
<th>Spring Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 101 Intro to Business</td>
<td>CS 310 Database Programming</td>
</tr>
<tr>
<td>CS 365 The 3 C’s: Cybercrime, Cyberlaw, and Cyberethics</td>
<td>CS 350 Management of Cybersecurity</td>
</tr>
<tr>
<td>CS 345 Principles of Cybersecurity</td>
<td>CS 370 Network Defense Countermeasures</td>
</tr>
<tr>
<td>CS 375 Linux Operating Systems and Security</td>
<td>CS 388 Cyber Defense II</td>
</tr>
<tr>
<td>Gen-Ed Social Science</td>
<td>Gen-Ed Humanities</td>
</tr>
<tr>
<td><strong>15</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>

*Completion of the General Education competencies by the end of the junior year.*

### Junior Summer

<table>
<thead>
<tr>
<th>Course</th>
<th>Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 441 Internship II</td>
<td>Fall</td>
</tr>
</tbody>
</table>

### Senior Year

<table>
<thead>
<tr>
<th>Fall Semester</th>
<th>Spring Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen-Ed Humanities</td>
<td>CS 448 Incident Response and Contingency Planning</td>
</tr>
<tr>
<td>CS 428 Penetration Testing</td>
<td>CS 488 Cyber Defense III</td>
</tr>
<tr>
<td>CS 438 Network Forensics</td>
<td>Major Elective</td>
</tr>
<tr>
<td>BS 201 Principles of Accounting I</td>
<td>IS 461 Seminar of Faith and Life</td>
</tr>
<tr>
<td>Major Elective</td>
<td>Gen-Ed Humanities</td>
</tr>
<tr>
<td><strong>15</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>

*Completion of 33 credits at the 300-level or above.*

Total hours required for degree: 126
Cybersecurity Minor

Requirements for a Minor in Cybersecurity (18 credits)

Cybersecurity Minor Core (15 credits)
- CS 207 Principles of O. S. and Comp. Hardware (3)
- CS 215 Introduction to Computer Networking (3)
- CS 335 Computer and Systems Security (3)
- CS 345 Principles of Cybersecurity (3)
- CS 350 Management of Cybersecurity (3)

Cybersecurity Minor Required Electives (3 credits)
Choose 3 hours from the following:
- CS 289 Cyber Defense I (2)
- CS 341 Internship I (3)
- CS 365 The 3 C’s: Cybercrime, Cyberlaw, Cyberethics (3)
- CS 370 Network Defense and Countermeasures (3)
- CS 375 Linux Operating Systems and Security (3)
- CS 380 Certification Study and Preparation (3)
- CS 428 Penetration Testing (3)

- CS 448 Incident Response & Contingency Planning (3)
- CS 475 Cybersecurity Program and Strategies (3)
- CS 488 Cyber Defense (4)
COMPUTER STUDIES (CS)

CS 102  Computer Applications and Concepts (3)
This course will enable students to improve their skills as knowledge workers with an emphasis on personal productivity concepts through using functions and features in computer software such as word processing, spreadsheets, presentation graphics, communications and scheduling, and online learning systems. This course provides an overview of microcomputer applications including a brief introduction to computer concepts, Microsoft Windows 7, Outlook 2013, Word 2013, Excel 2013, PowerPoint 2013 and Moodle, an online learning management system. (8 weeks)

CS 102E  Computer Competency Exam (3)
An examination to fulfill the computer competency requirement. Credits given if student passes exam with the equivalent of a C grade or better.

CS 204  Fundamentals of Information Systems (3)
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. Pre-requisite: CS 102 or permission of professor. (8 weeks)

CS 207  Principles of Operating Systems and Computer Hardware (3)
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. Pre-requisites CS 204.

CS 215  Introduction to Computer Networking (3)
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. Pre-requisite: CS 207.

CS 221  Introduction to Secure Programming Logic (3)
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. Pre-requisite: CS 204 or permission of professor.
CS 280  Special Topics in Computer Studies (Lower-Level) (1-3)
This course will provide students and faculty the opportunity to examine current issues or specialized topics within the discipline at a lower-level of study (appropriate for freshmen or sophomore academic experience). Topics will be determined by the department. Class will meet 15 hours for each hour of credit offered. Repeatable for different topics. *(Offered by department discretion.)*

CS 287  Cyber Competition I (2)
This course, open to freshmen and sophomores, prepares students to be part of a cyber competition such as the National Cyber League (NCL) or similar. Said competitions can be ‘offensive’ in nature (Capture the Flag etc.). *Pre-requisite: permission of professor.*

CS 289  Cyber Defense I (2)
This course, open to freshmen, sophomores and juniors, prepares students to be part of a Cyber Defense competition such as the Southeast Collegiate Cyber Defense Competition, SECCDC. *Pre-requisite: Permission of professor.*

CS 310  Database Programming (3)
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. *Pre-requisite: CS 302 or permission of professor. (Offered every spring)*

CS 335  Computer and Systems Security (3)
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 risk and 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 215.*

CS 341  Internship I (3)
Supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with information systems, information technology, information security or cybersecurity. *Pre-requisite: IS 310, sophomore standing or permission of professor. (Offered by department discretion)*

CS 345  Principles of Cybersecurity (3)
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. *Pre-requisite: CS 335.*

CS 350  Management of Cybersecurity (3)
Detailed examinations of a systems-wide 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 security practices, security architecture and models, continuity planning and disaster recovery planning. *Pre-requisite: CS 345.*
The 3 C's: Cybercrime, Cyberlaw and Cyberethics (3)
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.

Network Defense and Countermeasures (3)
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. Pre-requisite: CS 345.

Linux Operating Systems and Security (3)
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. Pre-requisite: CS 215.

Certification Study and Preparation (3)
The Cybersecurity concentration is optimally designed to equip our graduates with the necessary skills and knowledge to enter the IT workforce. This course will assist students who plan to study and prepare for IT certifications in A+ or Network+ or Security+ or Linux. Pre-requisites: CS 207 or CS 215 or CS 335 or CS 375.

Cyber Competition II (2)
This course prepares sophomore or junior status students who are returning participants to compete in a cyber-competition such as the National Cyber League (NCL). Said competitions can be ‘offensive’ in nature (Capture the Flag etc.). Pre-requisite: CS 287 or permission of professor.

Cyber Defense II (2)
This course prepares sophomore or junior status students who are returning participants to compete in a cyber-defense competition such as the Southeast Collegiate Cyber Defense Competition (SECCDC) or similar. To promote teamwork and leadership, students may serve as sub-team (Windows, Linux, Firewall and Incident Response etc.) leads. Pre-requisite: CS 288 or permission of professor.

Penetration Testing (3)
A detailed examination of real world cybersecurity knowledge, enabling recognition of vulnerabilities, exploitation of system weaknesses, and safeguards against threats. 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 370 or permission of professor.

Network Forensics (3)
In this course, students will learn to identify network security events, incidents, intrusions and sources of digital evidence in a lab environment. 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 428 or permission of professor.
CS 441  Internship II (3)
Supervised internship provides students with the opportunity to integrate classroom instruction with on-the-job training in an area associated with cybersecurity. **Pre-requisites: IS 310, CS 341, junior standing, permission of department. (Offered by department discretion)**

CS 448  Incident Response and Contingency Planning (3)
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. **Prerequisite: CS 370 or permission of professor.**

CS 475  Cybersecurity Programs and Strategies (3)
This course integrates learning from all prior CS courses, encourages the student to develop skills in synthesis and communication both written and oral, and teaches new material about the role of the CISO and the strategic and tactical planning and operation of the cybersecurity department in a variety of organizations. A research paper will be prepared and presented in the course. Outside speakers will supplement the course and provide the student additional, outside perspectives on the cybersecurity industry. **Prerequisite: CS 448 or permission of professor.**

CS 480  Special Topics in Computer Studies (Upper-Level) (1-3)
This course will provide students and faculty the opportunity to examine current issues or specialized topics within the discipline at an upper-level of study (appropriate for junior or senior academic experience). Topics will be determined by the department. Class will meet 15 hours for each hour of credit offered. Repeatable for different topics. **Prerequisites: CS 102, CS 204. (Offered by department discretion.)**

CS 487  Cyber Competition III (2)
This course prepares junior or senior status students who are returning participants to compete in a Cyber competition such as the National Cyber League (NCL) or similar. Said competitions can be ‘offensive’ in nature (Capture the Flag etc.). To promote leadership and teamwork, students may serve as vice-team captain or team captain of the competition. **Prerequisites: CS 387 or permission of professor.**

CS 489  Cyber Defense III (2)
This advanced cyber defense preparation course prepares junior or senior status students who are returning participants to compete in a cyber-defense competition such as the Southeast Collegiate Cyber Defense Competition (SECCDC) or similar. To promote leadership and teamwork, students may serve as sub-team lead, vice-team captain or team captain of the competition. **Prerequisites: CS 388 or permission of professor.**