Bachelor of Science in Cybersecurity Major

Dr. Adam Beatty, Program Director

Cybersecurity Program Mission

The mission of the B.S. in Cybersecurity is to prepare graduates with the ability to apply learned skills and experiential knowledge of security technology to make a significant contribution to the information security of individuals, corporations, governmental services and the national community.

Program Description

The Bachelor of Science in Cybersecurity is a 2-year, online degree-completion program that can be taken full time or part time and is designed for working adults who already have some college credit. Graduates will be prepared to contribute to and lead others in the quickly evolving dimensions of Information Technology (IT) related to cybersecurity. The Program provides opportunities for students to acquire the knowledge, skills, and experience necessary for demonstration of competency in the field of cybersecurity at the baccalaureate level.

Graduates will be prepared to contribute to and lead others in the quickly evolving dimensions of technology related to cybersecurity.

Graduates will be prepared to conduct the seven main categories of cyber operations as defined by the National Cybersecurity Workforce framework. They will be able to: (1) securely provision, (2) operate and maintain, (3) protect and defend, (4) investigate, (5) collect and operate, (6) analyze, and (7) provide oversight and development. Simplified, graduates will be prepared for a variety of careers in the rapidly growing industry of cybersecurity.

The National Cybersecurity Workforce Framework and U.S. Department of Labor have identified potential job opportunities for graduates of cybersecurity programs that include, but are not limited to:

- Information Security Analyst
- Information Systems Security Engineer
- Intrusion Detection System (IDS) administrator, engineer, or technician
- Network Administrator
- Computer Crime Investigator
- Cyber Trainer
- Chief Information Security Officer (CISO)

Program Outcomes

The graduate will:

1. Establish and supervise legal and ethical practices in the cybersecurity arena;
2. Develop and implement a comprehensive cybersecurity strategic plan

for individuals, corporations, governmental agencies, or the national community;

3. Detect, assess, and remediate ongoing cybersecurity threats and vulnerabilities;
4. Effectively communicate cybersecurity threats and remediation strategies across organizational levels in both verbal and written formats; and
5. Integrate knowledge, software and hardware capabilities, and threat and vulnerability awareness across varying technology formats, such as operating systems, networking, social media, mobile and handheld devices.

What You Will Study

Students in the Cybersecurity program complete foundational courses (24 credits), Cyber required courses (33 credits), Organizational Leadership required courses (18 credits), and general electives (45 credits), for a total of 120 credits.

Foundational Courses (24 credits)*	
Course	**Credits**
ENGL 101: Freshman Writing I	3
ENGL 102: Freshman Writing II	3
SPCH 103: Oral Communication Fundamentals	3
SSCI 105: Issues in Social Science	3
HIST 211 or 212: World Cultures I or World Cultures II	3
HUMN 110: Unheard Voices	3
NSCI 117: Why Science Matters	3
MATH 116 or 120: Intermediate Algebra	3
Total	**24**

* Some foundational course requirements may be met with transfer credits; this will vary by student.

B.S. Cybersecurity Major Courses (33 credits)	
Course	**Credits**
CYBR 100: Intro to Computers (or A+ Certification)	3
CYBR 110: Intro to Networking (or Network + Certification	3
CYBR 120: Intro to Security (or Security + Certification)	3
CYBR 310 Cybersecurity Strategy	3
CYBR 320 Ethical Hacking & Countermeasures (Certified Ethical Hacker)	3
CYBR 330 Incident Handler	3
CYBR 340 Security Analysis	3
CYBR 410 Certified Information Systems Security Professional - Phase I	3
CYBR 415 Certified Information Systems Security Professional - Phase II	3
CYBR 440 Advanced Security Trends	3
CYBR 450 Cybersecurity Capstone	3
Total	**33**

Minor Electives (18 credits)	
Organizational Leadership Minor	
ORGL 151 Introduction to Business	3
ORGL 309: Collaborative Leadership	3
ORGL 402: Organizational Behavior	3
ORGL 430: Leading Teams: Practicum	3
ORGL 401: The Learning Organization	3
ORGL 406: Organizational Development & Change	3
Total	**18**
General Electives	**45**
Total credits for program	**120**

Transfer Credit

Undergraduate students enrolled in an undergraduate degree or certificate program must complete at least 25% of the total credits required for the program while in residence at the University of Charleston. The minimum residency requirement for a bachelor's degree is 30 credits.

Admission Requirements

Applicants must gain general admission to the university, have a 60-credit associate degree in Cybersecurity or another technology-related field from a regionally accredited college or university **or** have a minimum of 60 semester credit hours with the primary focus on technology. **The 60 credits must include 9 credits of prerequisite courses or certifications as noted below.** Applicants must have a minimum GPA of 2.0.

Additional Requirements

- Completion of all University of Charleston Foundation Course Outcomes;
- Completion of 120 credits, including transfer credit;
- Completion of 24 credits of Foundational Courses;
- Completion of 33 credits within UC's cybersecurity curriculum;
- Completion of 18 credits within UC's organizational leadership curriculum;