Cyber Security Major

The Bachelor of Science in Cyber Security prepares individuals for a career as a security professional. This curriculum prepares students for success in IT Security, Cyber Security, Information Assurance, and Information Security Systems Security. It is designed for students with some background in computers.

All major requirements must be completed with a grade of 'C' or higher.This major requires a minimum of 45 credits.

In order to earn a Bachelor's degree at Charter Oak, all Major, General Education, Liberal Arts , elective, and Upper Division credit must equal 120 or more credits.

Major Requirements

This major contains courses in both Information Technology and Computer Science. Please review those sections for more information on the courses below.

CSS 101: Cybersecurity Fundamentals	3cr
Operating Systems and Asset Security	3cr
Incident Response	3cr
ITE 115: Program Logic and Design with Python	3cr
ITE 220: Networking and Data Communications	3cr
CSS 146: Legal Issues in Information Security	3cr
CSS 345: Auditing IT Infrastructure for Compliance	3cr
CSS 346: Access Controls, Authentication and PKI	3cr
CSS 435: Fundamentals of Network Security	3cr
CSS 436: Systems Forensics, Investigations and Response	3cr
CSS 437: Hacker Techniques, Tools and Incident Handling	3cr
CSS 438: Security Strategies for Web Apps and Social Networking	3cr
Please choose ***two*** of the following: • CSS 347: Security Strategies in Windows OS/Applications • CSS 348: Security Strategies in Linux OS/Applications • CSS 448: Cyberwarfare • Cyber Security Internship	6cr
CSS 490: Capstone	3cr

Program Learning Outcomes

Students who graduate with a major in Cyber Security will be able to:

- explain the landscape, key terms, and concepts related to the many layers of information systems security;
- explore and explain the fields in digital forensics and cyber policy analysis;
- create policies and standard operating procedures for organizations that are ethically, morally, and legally sound while recognizing ethical dilemmas and social responsibilities;
- identify and critically assess issues and concepts related to the protection of information and information systems;
- use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions at risk in information systems; and
- illustrate and explain fundamental architectures of networks and the Internet, as well as their underlying principles.