Bachelor of Science

Cybersecurity

• CIP code 430116 • 120 credits

Program Description

The Bachelor of Science in Cybersecurity equips students with the practical and conceptual means to understand and navigate today's vast digital security landscape. This expansive program focuses on the National Initiative for Cybersecurity Education (NICE) identified skill sets for the Cybersecurity workforce. The curriculum aligns a wide variety of courses with the technical, legal, social, and investigatory aspects of digital security. Students will emerge with the competencies necessary to compete in a growing global market that demands highly skilled Cybersecurity professionals. Two distinct concentrations enables students to select a range of career paths that fits their interests and goals.

Program Outcomes:

Graduates of the Cybersecurity program will have demonstrated proficiency in the following areas:

- Techniques used to protect the integrity of an organization's security architecture and safeguard its data against attack, damage or unauthorized access
- Design and develop IT risk and cyber security programs using industry frameworks and methodologies
- Knowledge of cybersecurity regulatory environment and ethics
- Monitor and assess cloud assets and resources for misconfigurations and non-standard deployments
- Meeting the challenges of evolving cyber network threats

The Cambridge College Cybersecurity program is designed to provide the requisite skills and knowledge-base for successful graduates to sit for the following certifications: CompTIA (Cybersecurity Analyst) CSA, CompTIA (Information Security Specialist) Security+.

Careers and Further Study

A Bachelor's Degree in Cybersecurity from Cambridge College qualifies you for in-demand positions such as:

- Information Security Manager
- Cybersecurity Analyst
- Cybersecurity Consultant
- Network Administrator
- Security and Risk Compliance Analyst
- IT Auditor
- Penetration and Vulnerability Tester

Degree completion: General education requirements may be satisfied by an associate's degree or 60 credits of prior courses that meet all general criteria for transfer; up to 90 credits may be accepted.

General Education ..... 42 credits

LRN 175	Principles & Processes of Adult Learning	3
WRT 101	College Writing I	3
CTH 225	Foundations of Critical Thinking	3
MAT 101	College Math I	3
CMP 130	Introduction to Computer Applications	3
CMP 230	Information Literacy	3
WRT 102	College Writing II	3
MAT 102	College Math II	3

WRT 101-102 and MAT 101-102 may by waived if equivalent courses have been accepted in transfer. Credits will be replaced with open electives. WRT 201 required if both WRT 101-102 are waived; not required for students completing WRT 101-102 at Cambridge. WRT 090 and MAT 100 required if assessment indicates need.

Arts & Humanities 6
Natural & Physical Sciences 6
Social Sciences 6

Open Electives ..... 36 credits

Choose electives and/or concentrations to support your academic interests and professional goals.

Cybersecurity Major ..... 42 credits

Core courses ..... 27 credits

CMP 250	Fundamentals of Cybersecurity
CMP 255	Information Security Foundations
CMP 260	EndPoint & Infrastructure Security
CMP 270	Operating Systems, Applications & Services
CMP 280	Introduction to Computer & Network Security Essentials
CMP 300	Digital Forensics
CMP 341	Incident Response
CMP 350	Cybersecurity Communications
CMP 390	Emerging Technologies

Concentrations ..... 15 credits

Choose one concentration:

Network Security

CMP 400	Cloud Networking Security
CMP 401	Wireless Technology & Security
CMP 415	Network & Digital Forensics Investigation
CMP 435	Network Protection & Threat Monitoring
CMP 450	Machine Learning for Network Intrusion Detection

Information Security & Risk Management

CMP 302	Cybersecurity Governance Frameworks
CMP 323	Digital Law – Policies, Regulations, Ethics
CMP 331	Cybersecurity Audit & Risk Management
CMP 455	Protecting and Handling Data
CMP 460	Risk Response & Monitoring