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

LRN175	Principles & Processes of Adult Learning	3
WRT101	College Writing I	3
CTH225	Foundations of Critical Thinking	3
MAT101	College Math I	3
CMP130	Introduction to Computer Applications	3
CMP230	Information Literacy	3
WRT102	College Writing II	3
MAT102	College Math II	3

WRT101-102 and MAT101-102 may by waived if equivalent courses have been accepted in transfer. Credits will be replaced with open electives. WRT201 required if both WRT101-102 are waived; not required for students completing WRT101-102 at Cambridge. WRT090 and MAT100 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**

CMP250	Fundamentals of Cybersecurity
CMP255	Information Security Foundations
CMP260	EndPoint & Infrastructure Security
CMP270	Operating Systems, Applications & Services
CMP280	Introduction to Computer & Network Security Essentials
CMP300	Digital Forensics
CMP341	Incident Response
CMP350	Cybersecurity Communications
CMP390	Emerging Technologies

Concentrations................................... 15 credits

Choose one concentration:

Network Security

CMP400	Cloud Networking Security
CMP401	Wireless Technology & Security
CMP415	Introduction to Network & Digital Forensics Investigation
CMP435	Network Protection & Threat Monitoring
CMP450	Machine Learning for Network Intrusion Detection

Information Security & Risk Management

CMP302	Cybersecurity Governance Frameworks
CMP323	Digital Law – Policies, Regulations, Ethics
CMP331	Cybersecurity Audit & Risk Management
CMP455	Protecting and Handling Data
CMP460	Risk Response & Monitoring

All courses 3 credits except as noted