ecpi UNIVERSITY

COLLEGE OF TECHNOLOGY
MASTER OF SCIENCE IN CYBERSECURITY (MSCS)

CYBERSECURITY

In today's vastly connected world, cybercrime is an ever-present threat. At ECPI University, our Cybersecurity program offers the training and knowledge to mitigate such risks and provide secure information technology systems at enterprise levels.

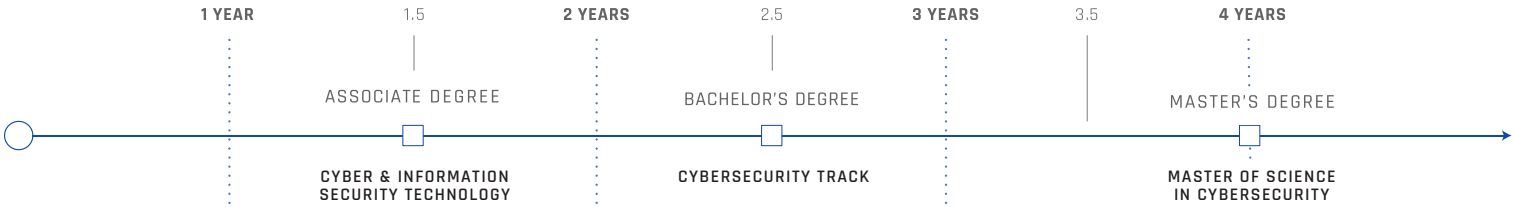
This program is ideal for aspiring IT professionals, executives, and baccalaureate degree graduates who are seeking theoretical, practical, and applied skills in computer-based information systems, as well as the technologies that support them.

You could earn your Master's degree in Cybersecurity at ECPI University in as little as 16 months!

Choose from two Cybersecurity tracks: Cyber Operations or Cybersecurity Policy:.

Cyber Operations focuses on the design, deployment, monitoring, and analysis of cyber technologies, and the techniques necessary to maintain security. Graduates of the Cyber Operations track will have the knowledge and skills required to ensure operational continuity of large-scale organizations.

Cybersecurity Policy prepares graduates for the development, enforcement, and analysis of security policies and procedures as related to people, processes, and technology. This course focuses on the legal and regulatory factors surrounding the administration of cybersecurity policy.



Outcomes

Graduates of the Cybersecurity degree program are able to analyze structured network communications, securely implement large-scale distributed cloud systems, evaluate possible threats and consequences to mitigate risks, and devise defensive network architecture.

Possible Career Track

Possible job titles for an M.S. Cybersecurity graduate include:

- Cyber Security Analyst
- Data Center or Network Security Administrator
- Risk Assessment and Vulnerability Analysis Manager
- Penetration Tester
- Information Systems Security Engineer

CYBERSECURITY
MASTER OF SCIENCE DEGREE

To receive the Master of Science in Cybersecurity, student must earn 36 semester credit hours. Required courses to be taken by everyone admitted to the program, include seven core courses (24 credit hours). Core courses build upon the knowledge support courses or appropriate experience. The program requires a minimum of four semesters, 15 months or 60 weeks of instruction.

Program Requirements are as follows:

CORE CURRICULUM 24 SEMESTER CREDIT HOURS	CREDITS
Cybersecurity Synopsis	3
Security Architecture & Design	3
Secure Coding Python	3
Cloud Security	3
Network Security and Next-Gen Firewalls	3
Wireless, Mobile, and IoT Security	3
AI/Machine Learning and Cybersecurity	3
Cyber Defense Capstone	3

CYBEROPERATIONS CONCENTRATION 12 SEMESTER CREDIT HOURS	
Applied Cryptography and Data Protection	3
Advanced Networking	3
Hardening Enterprise Cybersecurity Architecture: A Management Approach	3
Cyber Forensics	3

CYBERSECURITY POLICY CONCENTRATION 12 SEMESTER CREDIT HOURS	
Information Risk Management	3
Cybersecurity Governance and Compliance	3
Cybersecurity Strategies (Prevention and Protection)	3
Compliance and Audit	3

SEMESTER CREDIT HOURS	36

*These are the courses making up the degree plan at the time of student enrollment. The University at its sole discretion may modify the program track as deemed necessary.