MASTER OF SCIENCE IN CYBERSECURITY

Program Contact: Frederick Scholl (frederick.scholl@qu.edu)
203-582-7394

The Master of Science in Cybersecurity program is a program within the School of Computing and Engineering. The program is offered fully online, or hybrid online/on-ground. It is a technical degree program designed to prepare a wide range of students to operate as cyber defenders for present-day and future information systems and networks.

The 30-credit Master of Science in Cybersecurity includes up-to-date security knowledge and skills in demand in today's workplace. These include principles of risk management, software security, cloud security and resilient systems. Both security theory and hands-on skills are developed, utilizing current security tools in cloud and on-ground environments. The program and university meet the requirements for the NSA/DHS Center of Academic Excellence in Cyber Defense (CAE-CD) designation. Degree coursework culminates with a capstone project that challenges students to examine the architecture of a complex system, identify vulnerabilities and determine the specific security defenses that should be employed.

Master of Science in Cybersecurity Program of Study

The following courses are core requirements of the Cybersecurity program:

Code	Title	Credits
CYB 505	Introduction to Cybersecurity	3
CYB 510	Introduction to Security Technology	3
CYB 550	Cyber Policy	3
or CYB 613	Practical, Hands-On Healthcare Cyber Risk Management	
or CYB 617	Introduction to Cybersecurity Risk in Fin Tech	
CYB 520	Concepts and Practices for Securing Data	3
CYB 530	Programming for Security Professionals	3
CYB 615	Introduction to Ethical Hacking Operational Reconnaissance, and Penetration Testing.	3
CYB 690	Introduction to Secure Authentication And Access	3
CYB 695	Cloud Security	3
CYB 696	Introduction to Designing, Testing, and Operating Resilient Systems	3
CYB 691	MS Cybersecurity Capstone	3

Student Learning Outcomes

The mission of the MS in Cybersecurity program is to equip students to succeed as effective cyber defenders in a rapidly changing business and technology environment. Specific objectives include:

1. **Train** students to be able to apply risk management concepts to cybersecurity challenges.
2. **Enable** students to use and evaluate software to manage cybersecurity risk.
3. **Create** the next generation of cloud native security professionals.
4. **Enable** students to design, build and operate resilient systems that meet business objectives.

Admission

To qualify for admission into the MS Cybersecurity program, a student must have completed a bachelor's degree from a regionally accredited institution and meet *one of the following criteria*:

1. Have an undergraduate degree in computer engineering, software engineering or computer science; OR
2. Have an undergraduate degree in another area with applicable coursework or certificates in network technology, database management and programming; OR
3. Have at least 2 years of applicable work experience or military service including experience with network technology, database management and programming; OR
4. Receive approval from the program director