Cybersecurity - Information Assurance

Graduate Certificate
18 Credit Hours

This program is offered by the George Herbert Walker School of Business and Technology. It is available online, at the St. Louis main campus and at select campus locations. Please see the Campus Locations and Offering section of this catalog for a list of campuses where this program is offered.

For information on the general requirements for a certificate, see Certificate Program Policies and Procedures under the Academic Policies section of this catalog.

Program Description

This certificate focuses on expanding the student's knowledge and understanding of the cybersecurity challenges and issues facing corporate and governmental organizations. Courses in the certificate provide an understanding of current cybersecurity threats, phraseology and terminology, various roles, responsibilities, and processes applied in protecting an organization's digital content, as well as evaluation of transmission media, storage systems, networks, risk management and national critical infrastructure. The primary goal of this certificate program is to support IT/CS professionals seeking to expand their understanding of the cybersecurity discipline and to apply that knowledge to their profession.

This cybersecurity certificate program is intended for computer science, information technology, information security and related experienced professionals with the goal of expanding their understanding of cybersecurity policies, practices, methods and related technology advancements within the discipline. **This certificate program is NOT intended for students without an undergraduate degree and/or professional experience in these disciplines.**

Learning Outcomes

- Summarize and demonstrate an understanding of the vocabulary of cybersecurity terms and phraseology.
- Develop an understanding of the cyber threats to national critical infrastructure.
- Demonstrate and differentiate a basic working knowledge and awareness of current and growing threats to people, organizations and society through the use of cyber war, cyber crime, encryption techniques and other activities.
- Explain the basic knowledge of potential threats and how criminals and nation-states use different cyber techniques, the use of encryption methods and managing cyber risks.
- Describe the roles, responsibilities and duties of computer scientists, IT managers, CIOs, CEOs and other decision makers who may influence the use of IT systems.
- Differentiate the scope of the evolving environment of cybersecurity, international law, national law enforcement and organizational security measures and counter measures as applied to network and telecommunications operational security and applications.

Requirements

- CSSS 5110 Cybersecurity Communications (3 hours)
- CSSS 5120 Cybersecurity Infrastructures (3 hours)
- CSSS 5140 Cybersecurity Strategic Operations (3 hours)
- CSSS 5160 Encryption Methods and Techniques (3 hours)
- CSSS 5270 Cybersecurity in Cloud Computing (3 hours)
- CSSS 5290 Cybersecurity Risk Management Framework (3 hours)

NOTE: CSSS 5000 is not a prerequisite requirement for this certificate.

Admission

See the Admission section of this catalog for general admission requirements. Students interested in applying must submit their application online at www.webster.edu/apply. Transcripts should be sent from your institution electronically to transcripts@webster.edu. If this service is not available, send transcripts to:

Office of Admission
Webster University
470 E. Lockwood Ave.
St. Louis, MO 63119