Master of Cybersecurity

Program Outcomes: What Will I Learn?

1. Continuously monitor, maintain, and enhance the protection of enterprise-wide information assets through effective industry accepted information management and risk management techniques.
2. Detect, analyze and respond to cyber-attacks on networks and computer systems.
3. Conduct risk and vulnerability assessments of existing and proposed information systems.
4. Utilize the best sources of information available related to cyber security issues, threats, and recovery.
5. Demonstrate the ability to understand professional, ethical, and social responsibility, including the effect on culture, diversity, and interpersonal relations.
6. Demonstrate proficiency in communicating technical information in formal reports, documentation, and oral presentations to users and information technology professionals.
7. Demonstrate a commitment to professional development and to continue to engage in lifelong learning.

The revisions to this went into effect in July 2016, and the capstone course did not premiere until February 2017. Currently, this program does not have sufficient results to present outcomes data at the program level. Data represented on this site includes information on programs that have been in existence longer than 3 years, and have available direct and indirect learning outcomes data on at least 20 students, or unless otherwise specified by specialized accreditation to require reporting of all results less than n = 20.