Cybersecurity (MS) w/emph in Data Analytics

This program is offered by the George Herbert Walker School of Business & Technology and is available online via asynchronous modality.

Program Description

Education at the graduate level is an expansion of the knowledge attained from undergraduate studies. Graduate education encourages the development of advanced skills, theoretical knowledge and critical thinking skills to practice the art and science of cybersecurity techniques to defend networks and systems, analyze attacks, and conduct forensic evaluations.

Students entering the cybersecurity program must have an undergraduate degree in Computer Science, Management Information Systems, Information Technology, or a related degree with an understanding of basic software programming, network management, and systems/development operations. Professional experience may be accepted upon evaluation. Additionally, it is important for the student to be proficient in written and oral communication skills.

The master of science (MS) in cybersecurity with emphasis in data analytics prepares individuals for demanding positions in public and private sectors analyzing, managing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks.

Students will be well-versed to apply their knowledge and critical thinking related to social engineering techniques, network defenses, online malware methods, critical infrastructure protection, fraud, theft, digital forensics, and threat detection.

The data analytics emphasis focuses on developing and applying data analytics skills to fulfill significant needs in the business community. Students will integrate business concepts as well as key methods and tools for large-size data modeling, analysis and solving challenging problems involving "Big Data."

Students may not apply for dual majors because of the technical nature of this MS degree program. Students may apply for sequential degrees as long as they do not duplicate core courses.

Learning Outcomes

Core Cybersecurity curriculum:

- Capable of explaining important technical methods and theories used throughout the discipline of cybersecurity.
- Capable of applying knowledge in the field of cybersecurity to analyze software and online issues.
- Capable of effectively integrating knowledge in the field of cybersecurity to propose solutions to real-world problems.
- Apply cybersecurity social engineering techniques, as well as deterrence and forensic analysis, to information systems, applications and operation situations.

Data Analytics emphasis:

- Explain the role of data analytics in organizational decision making.
- Compose query statements to implement the data definition and manipulation, and construct multidimensional data cubes analysis.
- Apply effective methods for analyzing, presenting and using informational data.
- Develop meaningful reports and visualization of business data analytics appropriate to a technical and non-technical audience.
- Articulate forecasting and predictive models for real-world analytical applications.

Program Curriculum

The 39 credit hours required for the MS in cybersecurity must include the 21 required core courses and the 18 required emphasis courses.

Core Courses (21 hours)

- CSSS 5100 Secure Software Design and Threat Analysis (3 hours)
- CSSS 5120 Cybersecurity Infrastructures (3 hours)
- CSSS 5160 Encryption Methods and Techniques (3 hours)
- CSSS 5180 Social Engineering (3 hours)
- CSSS 5220 Cybersecurity Threat Detection (3 hours)
- CSSS 5230 Cybersecurity Forensics (3 hours)
- CSSS 6000 Practical Research in Cybersecurity (3 hours)

Data Analytics Emphasis Courses (18 hours)

- BUSN 5760 Applied Business Statistics (3 hours)
- CSDA 5110 Analytics Programming with R (3 hours)
- CSDA 5210 Databases and Data Warehouses (3 hours)
- CSDA 5310 Data Visualization (3 hours)
- CSDA 5320 Analytics Applications using Python (3 hours)
- CSDA 5330 Data Mining (3 hours)