PROGRAM DESCRIPTION

Graduates from the M.S. in Cybersecurity will be prepared to become leaders and technical managers in cybersecurity, with a solid understanding of security technology and organizational management principles and practices, preparing them to make knowledgeable and responsible decisions.

M.S. in Cybersecurity students are prepared to become leaders and technical managers in cybersecurity, which requires solid understanding of security technology and organizational management principles and practices in order for graduates to make sensible and responsible decisions. Additionally, the EIU Cybersecurity program is designed to prepare graduates to take relevant certification exams, specifically CISCO Certified Systems Security Professional (CISSP), the COMPTIA A+, and COMPTIA Security+. According to the National Initiative for Cybersecurity Education (NICE), are requisites for entering and performing successfully in the cybersecurity profession.

According to the Bureau of Labor Statistics, the employment opportunities for Information Security Analysts is expected to increase at a much higher than average rate over the next decade, at 18% from 2014-2024. Similarly, The Illinois Department of Employment Security projects over 30% growth in the profession from 2012-2022. There is significant and growing demand for professionals with an information security background, and not enough supply of graduates to meet this demand. The M.S. in Cybersecurity is designed for working professionals with a general information technology background to specialize in this growing field to help to fill the projected demand for security expertise and to provide accessible professional growth opportunities for Illinois professionals and those from other areas interested in cybersecurity.

Typical positions will include (but are not limited to):

- Cybersecurity Consultant
- Network Security Specialist
- Information Assurance Specialist
- Computer Security System Analyst
- Web Security Engineer

- Information Security Officer
- Information Security Operations Manager
- Cybersecurity Administrator
- IT Security Manager

PROGRAM OBJECTIVES

1) Assess, by analyzing technical and operational requirements, an enterprise level information cybersecurity system.

2) Construct the architecture of a typical cybersecurity system; identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.

3) Conduct network penetration tests, troubleshoot, and implement attack countermeasures in a typical information system.

4) Identify the components of cybersecurity layered structure for:

   - Network defense architecture
   - Access control and auditing
   - Continuous network monitoring
   - Real-time security solutions

5) Describe and apply the fundamental and advanced technologies, components, and issues related to communications, data networks, and information systems.

6) Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management, for wired and wireless networks that affect security of the cyberspace.

Cybersecurity Coursework

Course	**Credits**
1: TEC 5313 - Networking and Advanced Data Communications	3
2: TEC 5323 - Advanced Database Technology	3
3: TEC 5353 - Cybersecurity	3
4: MIS 4850 - Systems Security	3
5: TEC 5363 - Database Security and Reliability	3
6: AET 4823 - Facilities Security	3
7: CYB 5550 - Cybersecurity Professional Seminar	3
8: MBA 5670 - Management of IT	3
9: TEC 5413 - Biometric Security	3
10: MIS 4860 - Ethical Hacking and Network Defense	3
11: CYB 5900 - Cybersecurity Capstone	2
Total Required Hours	**32**