Certificate in Cybersecurity Management

Program / Student Learning Outcomes: What Will I Learn?

Graduates of the Certificate in Cybersecurity Management will be able to:

1. Apply effective information security techniques to monitor, maintain, and enhance the protection of enterprise-wide information assets.
2. Implement an Incident Response team that legally, ethically, and efficiently responds to cyber incidents.
3. Detect, analyze, and respond to cyber-attacks on networks and computer systems.
4. Conduct risk and vulnerability assessments of existing and proposed information systems.
5. Utilize the best sources of information available related to cyber-security issues, threats, and recovery.
6. Apply strategies to build relationships with other Incident Response teams, organizations, and law enforcement to improve incident response effectiveness.

Assessment Methodology

Metrics, Assessments, and Levels of Achievement

The table below provides a brief overview of the measures selected to assess program outcomes for the Certificate in Cybersecurity. Assessment of program/student outcomes consists of one direct measure, which is assessed in the capstone course. Benchmarks have been established to differentiate between three levels of program/student outcome achievement (exceeds expectations, meets expectations, and does not meet expectations). These three levels of achievement are color coded and used in the section below to indicate the level of achievement for each measure, for each learning outcome.

Metric Type	**Direct Measures**
Assessments	Capstone Portfolio: CYS590 Special Topics in Cybersecurity
Metrics	The percentage of students received a 2 (out of three) or higher on the learning statements and supporting evidence for the related student outcome.
Exceeds Expectations	≥ 85%

Meets Expectations	70 - 84%
Does Not Meet Expectations	< 70%

Note: Due to the small number of students who have taken the capstone course, data were aggregated from March 2014 to August 2016 to in order to have enough information to warrant a meaningful analysis.

Key:

Result
N

Program/Student Outcome Achievement Results

July 2013 Term to August 2016 Term

Program / Student Learning Outcome 1

Apply effective information security techniques to monitor, maintain, and enhance the protection of enterprise-wide information assets.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12

Program / Student Learning Outcome 2

Implement an Incident Response team that legally, ethically, and efficiently responds to cyber incidents.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12

Program / Student Learning Outcome 3

Detect, analyze, and respond to cyber attacks on networks and computer systems.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12

Program / Student Learning Outcome 4

Conduct risk and vulnerability assessments of existing and proposed information systems.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12

Program / Student Learning Outcome 5

Utilize the best sources of information available related to cyber-security issues, threats, and recovery.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12

Program / Student Learning Outcome 6

Apply strategies to build relationships with other Incident Response teams, organizations, and law enforcement to improve incident response effectiveness.

Direct Measure	
CYS590 Special Topics in Cybersecurity	100%
	n = 12