Master of Science in Cybersecurity, M.S.

The Master of Science in Cybersecurity is intended for individuals who desire to acquire additional cybersecurity knowledge, skills, and abilities in order to pursue new or advance existing careers in cybersecurity. The program is also designed for individuals who plan to pursue doctorate degrees in cybersecurity or related fields. The program focuses on the managerial and technical perspectives of cybersecurity through extensive use of case-studies and hands-on lab exercises.

Matriculation Requirements

1. Bachelor's degree with a GPA of at least 3.2 on a 4.0 scale from an accredited institution in one of the following fields: (Applicants who have bachelor's degrees in other fields may be admitted to the program if they have at least two years of technology or cybersecurity industry experience and have completed undergraduate courses in data communication, programming, and server administration with a grade of C+ or better. Students may also take a comprehensive exam on these topics to satisfy this admission requirement. These applications will be handled on a case-by-case basis.)
2. Information Systems
3. Information Security
4. Information Technology
5. Computer Science

2. Admission Essay

3. Completed application for admission

4. Official transcripts from all attended institutions of higher education

5. Two letters of recommendation

Program Requirements

Code	Title	Credit Hours
Total Credit Hours		**30**
Discipline Core Requirements		**21 Credits**
Complete the following required courses:		
IT 6300	Principles of Cybersecurity	3
IT 6330	Cybersecurity Operations	3
IT 6350	Law/Ethics/Privacy in Cybersecurity	3
IT 6370	Penetration Testing and Vulnerability Assessment	3
IT 6740	Advanced Network Defense and Countermeasures	3
IT 6770	Cybersecurity Management	3
IT 6900	Cybersecurity Capstone	3
Elective Requirements		**9 Credits**
Complete 9 credits from the following:		9
IT 6660	Advanced Network Forensics (3)	
IT 6750	Reverse Engineering and Malware Analysis (3)	
IT 6780	Secure Coding (3)	
INFO 6420	Web and Mobile Application Security (3)	
or other departmental approved electives.		

Graduation Requirements

1. Complete all courses with a grade of B- or better with an overall GPA of 3.0 or higher.
2. Courses must be finished within a five-year period. No courses will apply toward graduation that are older than five years.

Graduation Plan

This graduation plan is a sample plan and is intended to be a guide. Your specific plan may differ based on your Math and English placement and/or transfer credits applied. You are encouraged to meet with an advisor and set up an individualized graduation plan in Wolverine Track (http://www.uvu.edu/wolverinetrack/).

First Year		
Semester 1		**Credit Hours**
IT 6300	Principles of Cybersecurity	3
IT 6330	Cybersecurity Operations	3
	Credit Hours	**6**
Semester 2		
IT 6740	Advanced Network Defense and Countermeasures	3
IT 6350	Law/Ethics/Privacy in Cybersecurity	3
	Credit Hours	**6**
Second Year		
Semester 3		
IT 6370	Penetration Testing and Vulnerability Assessment	3
IT 6770	Cybersecurity Management	3
	Credit Hours	**6**
Semester 4		
Elective		3
Elective		3
	Credit Hours	**6**
Third Year		
Semester 5		
IT 6900	Cybersecurity Capstone	3
Elective		3
	Credit Hours	**6**
	Total Credit Hours	**30**

Program Learning Outcomes

1. Demonstrate an understanding of the technical and managerial aspects of cybersecurity.
2. Demonstrate the ability to solve cybersecurity related problems and to make effective cybersecurity decisions in a dynamic and constantly changing environment.
3. Demonstrate proficiency in using the tools, techniques, and technologies related to the identification and mitigation of cybersecurity threats.
4. Develop an understanding of risk management methods as they relate to cybersecurity.
5. Develop an understanding of the legal, regulatory, and ethical issues surrounding cybersecurity.