

CYBERSECURITY, MS

Program Director: Hossein Sarrafzadeh, Ph.D.

Phone: 716-375-2089

Email: asarrafz@sbu.edu

Code	Title	Credits
Foundational Courses		
CYB-500	COMPUTER NETWORKS	3
Cybersecurity Core		
CYB-501	FOUNDATIONS OF CYBERSECURITY, ETHICAL HACKING, PENETRATION TESTING	3
CYB-502	ADVANCED CYBERSECURITY	3
CYB-503	Enterprise Security	3
CYB-504	CYBERSECURITY FORENSICS	3
CYB-505	SECURE SOFTWARE DESIGN	3
CYB-506	ENTERPRISE NETWORKS	3
CYB-507	APPLIED CRYPTOGRAPHY	3
CYB-508	APPLIED DATA MINING WITH APPLICATIONS IN CYBERSECURITY	3
CYB-509	MACHINE LEARNING WITH APPLICATIONS IN CYBERSECURITY	3
CYB-510	Risk Management & System Hardening & PROTECTION	3
Total Credits		33

CYB-500 COMPUTER NETWORKS (3 Credits)

A study of computer networks based on the OSI model of a layered network architecture. The TCP/IP protocol suite is used to illustrate network protocols. The course includes an overview of local area networks, routing algorithms, and network applications. The course consists of three lecture hours and one two-hour laboratory per week. The laboratory component provides experience in network programming using sockets.

Restrictions: RGP.123

CYB-501 FOUNDATIONS OF CYBERSECURITY, ETHICAL HACKING, PENETRATION TESTING (3 Credits)

To provide students with a fundamental understanding of cybersecurity and an in-depth understanding of penetration testing and ethical hacking. This course will include intelligence gathering, assessment of software vulnerabilities and weaknesses, cross platform penetration testing, learning ethical hacking requirements, and data protection.

Restrictions: RGP.123

CYB-502 ADVANCED CYBERSECURITY (3 Credits)

This course will expand on previous cybersecurity courses and delve deeper into its topics. Combining topics from computer science and cybersecurity, students will delve into system and network analysis, Diverse DDoS, DDoS and advanced persistent attacks, intrusion detection system development and control system. Students will be able to use quantitative and qualitative reasoning to solve problems with an array of different system vulnerabilities. Students will need knowledge of operating systems and advanced algebra before taking this course.

Restrictions: RGP.123

CYB-503 Enterprise Security (3 Credits)

This course will expand on previous cybersecurity courses and introduce business and enterprise topics. This will be done through analysis of real-world business examples of cyberattacks and the needs businesses have in the areas of cybersecurity. This course will emphasize real-world developmental practices and aim to improve students' ability to work in a professional cybersecurity environment.

Restrictions: RGP.123

CYB-504 CYBERSECURITY FORENSICS (3 Credits)

This course will give an in-depth look into the world of cybercrime and digital evidence. Throughout this course, students will use industry tools to perform forensic analysis of crimes to learn about how to prevent, detect, and respond to cyber-crime, cyber-terrorism, and cyber-predators.

This course aims to both inform students of the types of crimes that exist as well as ways to catch those responsible even through virtual anonymity.

Restrictions: RGP.123

CYB-505 SECURE SOFTWARE DESIGN (3 Credits)

This course aims to establish an understanding of proper software design for a secure product. This course will do so by comparing both secure and insecure design structures to ensure that similarly made software programs are not vulnerable to known forms of cyberattacks or cybercrimes.

Restrictions: RGP.123

CYB-506 ENTERPRISE NETWORKS (3 Credits)

This course will build an understanding of how networks function within a business environment and the threats that face networks if they are not properly protected. Networks are a cornerstone of a modern business of any size, and thus these networks must be made to be secure in order to ensure that these companies can function properly.

CYB-507 APPLIED CRYPTOGRAPHY (3 Credits)

This course will help students understand the fundamentals of cryptography as well as the applications that it holds in modern technology. Cryptographic methods and tools, such as encryption and digital signatures, will be studied to understand how to protect information within a program. This course will also explore the differences between symmetric and asymmetric cryptography and the benefits to both.

Restrictions: RGP.123

CYB-508 APPLIED DATA MINING WITH APPLICATIONS IN CYBERSECURITY (3 Credits)

This course will help students understand the importance of data mining in the cybersecurity field and how to apply various data mining techniques. Students will learn about the fundamentals to data mining in general, growing their skills until they are able to later integrate data mining into cybersecurity applications and topics.

Restrictions: RGP.123

CYB-509 MACHINE LEARNING WITH APPLICATIONS IN CYBERSECURITY (3 Credits)

This course will aim to enhance students' knowledge of the fundamentals of machine learning and how said technologies can be applied to cybersecurity. Different types of machine learning will be explored in the realms of cybercrime and cybercrime prevention.

Restrictions: RGP.123

CYB-510 Risk Management & System Hardening & PROTECTION (3 Credits)

This course will aim to teach students skills required to perform cyber risk management for organizations as well as how to prevent systems from being breached to begin with. There are risks that accompany all forms of system, this course will both give students the tools to identify possible risks that can be impactful in the future and how to manage breaches once they occur.

Restrictions: RGP.123