CYBERSECURITY, ADVANCED CERTIFICATE

Program Director: Dr. David Hilmey
Email: dhilmey@sbu.edu

Our graduate certificate in cybersecurity, available online only, provides an overview of the cybersecurity field that can complement your current work in a variety of fields including law enforcement, military, government agencies, and more. After completing these five courses you'll gain the confidence to speak the language and bring an understanding of the cybersecurity landscape to your current role.

Code	Title	Credits
CYB-500A	COMPUTERS & CYBER WORLD	3
CYB-500B	INTRODUCTION TO PROGRAMMING	3
CYB-500C	INTRODUCTION TO DATABASES	3
CYB-500	COMPUTER NETWORKS	3
CYB-511	FOUNDATIONS OF ETHICAL HACKING	3
Total Credits		**15**

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-500A COMPUTERS & CYBER WORLD (3 Credits)
Computer hardware and organization, number Systems, types of data, discrete mathematics and logic, algorithms, files and data structures, operating systems and compilers, virtual machines, Linux, security, privacy, threats, identity, introduction to technical, legal & policy issues in cybersecurity.

CYB-500B INTRODUCTION TO PROGRAMMING (3 Credits)
The course introduces the object-oriented approach to software design using a programming language such as Python, R or Java. The programming language is used to implement software designs. No previous programming experience is presupposed.

CYB-500C INTRODUCTION TO DATABASES (3 Credits)
An introduction to database management systems, including database design and application development. Different database models are introduced, with emphasis on the relational model. The theoretical principles underlying the design of a database and the physical storage of data and its integrity are covered. Other conceptual points are covered such as relations in mathematics that form the bases of a relational model. Along with designing and implementing databases using Sequel Server, the student will create a GUI interface to a database using JDBC and JavaFX.

CYB-501 SYSTEM ANALYSIS & INSTRUMENTATION (3 Credits)
This course will teach introductory but foundational requirements needed to understand and work in Windows and Linux shell environments. The technical skills covered in this course are prerequisite knowledge for forensics, investigation, and threat hunting work. The course will cover simpler PowerShell and Bash scripting, installing and configuring system monitoring, basic file system structures, basic intro to user and process environments, event logging, process types, and remote administration tools and techniques. This course will provide the requisite foundational knowledge for later technical courses in the Cybersecurity program.

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.
Restrictions: RGP.123

CYB-511 FOUNDATIONS OF ETHICAL HACKING (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-512 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.
Restrictions: RGP.123

CYB-515 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.
Prerequisite(s): #TAKE CYB-511 CYB-512
Restrictions: RGP.123

CYB-516 ADVANCED CYBERSECURITY THREATS (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-517 DIGITAL 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-518 ENTERPRISE RISK MANAGEMENT (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

CYB-519 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 unsecure software design structures to ensure that similarly made software programs are not vulnerable to known forms of cyberattacks or cybercrimes.
Restrictions: RGP.123

CYB-520 CLOUD SECURITY (3 Credits)
This course provides a practical explanation of both the principles and practice of cloud security by describing the cloud security architecture and exploring the guiding security design principles from the threat and CIA model viewpoint. In order to gain a thorough understanding of the design and development of secure cloud services we will examine industry standards and applied technologies for delivering and managing secure cloud-based services specially Google Cloud Platform (GCP). This course also covers protection and isolation of physical and logical infrastructures, identity management, access control, monitoring and auditing processes. Students also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.
Prerequisite(s): Take CYB-511
Restrictions: RGP.123

CYB-525 APPLIED DATA MINING 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-526 MACHINE LEARNING IN CYBERSECURITY (3 Credits)
Upon successful completion of this course, students will be able to apply a variety of learning algorithms and machine learning applications for enabling intelligent cybersecurity strategies. Having been equipped with machine learning fundamentals, the students can apply learning algorithms and train machines for face recognition, new generation of anti-viruses, vulnerability management, network security, authentication, anomaly detection, biometrics in cyber threats, etc.
Restrictions: RGP.123

CYB-527 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-535 CYBERSECURITY CAPSTONE (3 Credits)
Following a number of high-profile security breaches, your organisation has recognised the importance of developing a cybersecurity strategy. Stakeholders and management have asked you to present at the next board meeting. They've only allocated thirty minutes so they want you to record a presentation which clearly outlines the threats and risk to your organisation and your plan to address them. They also want you to explain how you plan to respond in the event of a data breach.