CYBERSECURITY (CYB)

CYB 123 Cybersecurity Threats and Defense
2 Class Hours, 2 Lab Hours, 3 Quarter Credit Hours
Prerequisites: NE 115
This course provides a broad overview of the field of cybersecurity. The course covers history, terminology and strategies involved in securing information assets and serves as a foundation course for more advanced studies in information, network and computer security. General and specific threats to information assets and defensive strategies for protecting those assets are covered. The course employs an integrated system of skill-building lessons, hands-on exercises, and self-assessment tools.

CYB 241 Security of the Internet of Things
2 Class Hours, 2 Lab Hours, 3 Quarter Credit Hours
Prerequisites: NE 255
In this course, students will explore the network of physical devices, vehicles, home appliances, and other items dubbed the Internet of Things. Students will learn about IOT by making their own networked devices using Raspberry Pi. The course will focus on highlighting how devices interact, share data and affect everyday life by combing a mixture of hardware, software.

CYB 242 Information Assurance, Policy and Compliance
3 Class Hours, 3 Quarter Credit Hours
This course introduces information assurance, cybersecurity policy development, legal compliance and lays a foundation for ethical decision-making by the cybersecurity professional. Students gain experience using non-technical measures to address cybersecurity threats to an organization. Cybersecurity professionals must be familiar with privacy and data protection requirements coming from HIPAA, FERPA, Sarbanes-Oxley, PCA and other federal and industry mandates. To better design penetration test scenarios, students are given the opportunity to work through ethically ambiguous scenarios that revolve around areas such as vulnerability discovery and responsible disclosure.

CYB 252 Cyber Scenarios
2 Lab Hours, 1 Quarter Credit Hours
Prerequisites: NE 255 and NE 121
This course focuses on the cyber threats landscape. It covers common cyber-attacks and what can be done to prevent them. The course utilizes virtual labs that allow students to examine and apply proper security controls to prevent common cyber-attacks. Students then apply knowledge gained to analyze and audit the result of a typical cyber-attack.

CYB 373 Ethical Hacking
2 Class Hours, 2 Lab Hours, 3 Quarter Credit Hours
Prerequisites: CYB 252
In this course, students will learn how to properly use techniques employed by professional penetration testers to validate information assurance. In addition to validation techniques, students will learn anti-hacking techniques, network reconnaissance tools, buffer overflows, password cracking and other concepts related to testing and validating network defenses.

CYB 394 Windows Security
2 Class Hours, 4 Lab Hours, 4 Quarter Credit Hours
Prerequisites: NE 381
Students will learn how to secure and troubleshoot a Microsoft Windows-based Active Directory network environment through an integrated system of skill-building lessons, hands-on exercises, and self-assessment tools.

CYB 408 Linux Security
2 Class Hours, 4 Lab Hours, 4 Quarter Credit Hours
Prerequisites: NE 385
This course builds on the Linux System Administration course, reacquainting students with administrative concepts and presenting security methodologies as they relate to Linux. It will present logical concepts and provide practical applications related to Linux and the applications and methodologies utilized to secure it. Discussions will include notable hacks, hardening topics and IP Tables, which is an internal firewall feature-set within Linux. Also, the course will present methods for securing both file and file systems. Upon completion of the course, students will have an understanding of Linux subsystems and their relationship to security through successful completion of the following labs: building both a Linux workstation and server; navigating the Linux file system; checking for rootkits; server block encryption; securing Apache; configuring IP tables (Linux Firewall); and hardening the OS.

CYB 409 Web Application Security
2 Class Hours, 2 Lab Hours, 3 Quarter Credit Hours
Prerequisites: NE 411
Students in this course will learn common security pitfalls in web applications as well as how to avoid them. Topics include use of encryption, spoofing, phishing, session management, secure data storage and other techniques related to ensuring the protection of the application and customer data.

CYB 412 Network Security
2 Class Hours, 4 Lab Hours, 4 Quarter Credit Hours
Prerequisites: NE 406
In this course, students will learn the fundamentals and skills related to network security. Topics such as IPSec, Network Access Control, network asset vulnerabilities, encryption techniques used on the Internet, security certificates, phishing, spoofing, browser configuration, network perimeter security and wireless network security are covered.

CYB 423 Incident Response
2 Class Hours, 2 Lab Hours, 3 Quarter Credit Hours
Prerequisites: CYB 394
Students will learn how to use forensic techniques in order to investigate and document system and network intrusions as well as malicious software incidents. System restoration techniques are also covered. Students will become adept at investigating advanced persistent threats, rogue employees, remote data breeches and other security violations.

CYB 426 Advanced Information Security
1 Class Hours, 4 Lab Hours, 3 Quarter Credit Hours
Prerequisites: CYB 394 and CYB 408
The Advanced Information Security course is designed to prepare students to take the CompTIA Security Plus (+) certification exam and Test Out Security Pro Certification. In this course, students cover information security best practices that all businesses should adhere to and learn how to implement information security best practices in business environments.

CYB 536 Network and System Information Assurance
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
The security threats and risks that govern computer systems and networks can be mitigated by using a variety of security models, mechanisms and protocols. Such mechanisms are used to implement security policies that are defined in a risk management strategy. Designing security architecture is a critical task that includes securing hardware, software and networks. This course introduces security models and the concept of subjects and objects in order to discuss authorization and access control. Case studies of how authentication and access control are implemented in real-life systems are also presented. Security risks that are related to networks are equally important. Students define secure communication channels and present known and established network security protocols (SSH, SSL, IPSec, etc.). Special cases such as wireless and mobile networks are also examined to demonstrate how traditional security architectures can be adapted to facilitate different requirements.

CYB 538 Security Auditing and Risk Management
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
In this course, students appraise all standards and information technology (IT) security audit processes, evaluate security controls, and examine governance of compliance and control responsibilities. Most organizations are required to comply with IT security regulations and/or standards resulting from the establishment of the Sarbanes-Oxley Act, General Computing Controls, the Gramm–Leach–Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), and the Payment Card Industry Data Security Standard (PCI DSS) Students will become familiar with these standards and regulations.

CYB 542 Ethical Hacking in Defense of the Enterprise
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
An ethical hacker is a security expert who attacks a system on behalf of the system's owners. This course focuses on discovering network vulnerabilities that a malicious hacker can exploit. The course explores penetration testing, footprinting and social engineering, scanning and enumeration, operating system weaknesses, and the methods used to hack web servers and wireless networks. Students perform hands-on projects using state-of-art hacking tools and techniques after extensive planning.

CYB 548 Robust Incident Response Planning
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
This course provides students with the background and skills to manage information security incidents to minimize impact on business operations. Topics include detection, investigation, and response to different types of security incidents. Students explore these topics by developing incidence response plans; utilizing industry-standard processes and tools for investigating information security incidents; and recommending processes for incidence response that adhere to legal, regulatory, and organizational compliance. Students who have completed the course have a comprehensive view of cybersecurity incident detection and response.

CYB 552 Digital Forensics & Breach Investigations
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
This course explores the expertise required to conduct digital forensic investigations. Topics include investigation methods, problem-solving techniques, current forensics analysis tools, digital evidence acquisition and control, and impact of ongoing technological changes on digital forensics. Student projects include scenario-based investigations in investigating cybersecurity breaches.

CYB 558 Secure Software Development
4 Class Hours, 4 Quarter Credit Hours
Prerequisites: MGM 533 (may be taken concurrently)
Software applications are often characterized as the cement of our times due to the high prevalence of computer systems in all aspects of our lives: banking, health, transportation, retail, even “smart home” systems. As a result, managing application security risks is a quite critical aspect of information security. This course aims to justify the importance of application security, firstly by analyzing how security can be integrated in the software development lifecycle. We demonstrate methods to identify vulnerabilities and discuss techniques that can be used to mitigate them and improve the overall security of software applications.