CBD 330 INTRODUCTION TO CYBER DEFENSE (3)

In this course, students learn the basic concepts, terminology, and technologies that comprise the field of cyber defense. Students in this course are introduced to topics such as risk/ threats in the cyber environment, threat assessment, cyber-defense terminology, cyber-defense planning, and general cyber-defense management.

Student Learning Outcomes

Students will:

1. Understand the fundamental concepts, terminology, and technologies of cyber defense.
2. Analyze and assess risks and threats in the cyber environment.
3. Develop foundational skills in planning and managing cyber defense systems.
4. Explore key elements of information security, including inspection, protection, and incident response.
5. Gain insight into legal, ethical, and professional issues in cybersecurity.

Course Topics

1. Foundations of Cyber Defense
2. The Need for Security
3. Legal, Ethical, and Professional Issues
4. Risk Management
5. Security Technologies
6. Cryptography
7. Physical Security
8. Implementing Information Se
9. Information Security Maintenance

CBD 332 CYBER DEFENSE NETWORKING (3)

Students in this course explore the fundamentals of network security and related topics. This course facilitates an understanding of the fundamentals of networking configurations and protocols, as well as threat and vulnerability recognition and mitigation from the perspective of the CIA triad: eavesdropping (confidentiality), man-in-the-middle (integrity), and denial-of-service (availability). Students will also engage in applied learning to reinforce lectures and provide practical implementation experience.

Student Learning Outcomes

Students will:

1. Evaluate key network risks and vulnerabilities.
2. Understand and apply security standards and models, including ISO and NIST frameworks.
3. Harden operating systems to defend against malware, network attacks, and other threats.
4. Deploy and manage network security measures, including firewalls and intrusion detection systems.
5. Protect data using encryption techniques, public/private key systems, and digital certificates.
6. Establish and enforce security policies to mitigate risks.
7. Prepare for post-incident investigations and manage responses to network breaches.

Course Topics

1. Network Defense Fundamentals
2. Risk Evaluation and Management
3. Security Technologies
4. Cryptography and Data Protection
5. Operating System Hardening
6. Security Policies and Standards
7. Incident Management

CBD 334 LEGAL AND ETHICAL ENVIRONMENT OF CYBER DEFENSE (W) (3)

In this course, students are exposed to the legal and ethical issues that relate to the field of cyber defense. In addition to learning about the laws and policies that shape and govern this field, students will also study topics such as General Data Protection Regulation (GDPR), the protection of information/ intellectual property, ethical hacking, and privacy concerns in public and private organization.

Student Learning Outcomes

Students will:

1. Understand the legal frameworks governing digital actions and cyber defense.
2. Analyze intellectual property laws and their implications in a digital age.
3. Explore U.S. and international privacy laws and their application in cyber defense.
4. Evaluate enterprise privacy concerns and strategies for compliance.
5. Gain hands-on knowledge of cyber defense team operations, including Blue, Red, and Purple Teams.

Course Topics

1. Cybersecurity Laws, Regulations, and Policies
2. Intellectual Property in the Digital Age
3. Privacy Laws and Regulations
4. Enterprise Privacy Concerns
5. Cyber Defense Team Operations
6. Ethical Hacking and Professional Responsibility

CBD 336 CYBER RISK MANAGEMENT AND MITIGATION (3)

This course explores cyber defense from a risk-management perspective. Students focus on strategies for assessing risk, as well as for implementing effective and proactive risk-management practices and risk-mitigation measures. Topics in this risk assessment include risk analysis, risk mitigation, risk management, networking components and Virtual Private Networks (VPN). Students will also learn about the resources and methods used for information assurance. The student will apply this knowledge to develop an assessment methodology and strategies for managing and mitigating risks in the cyber environment.

Student Learning Outcomes

Students will:

1. Understand the evolving cyber threat landscape and its impact on organizations.
2. Analyze and assess risks associated with cybersecurity using industry standards and methodologies.
3. Evaluate motivations of threat actors and types of vulnerabilities in systems.
4. Develop and implement effective cybersecurity controls and risk mitigation strategies.
5. Apply a risk-based approach to cybersecurity management.
6. Contrast and learn from high-profile data breaches to enhance risk management practices.

Course Topics

1. Digital Transformation and Cybersecurity
2. Data Breaches
3. Threat Actors and Events
4. Vulnerabilities
5. Cybersecurity Controls
6. Cyber Risk Management
7. Information Assurance Resources

CBD 451 PRACTICUM IN CYBER DEFENSE (3)

This is the capstone course for the major in cyber defense. This is an applied, lab-based class that provides students an opportunity to apply the knowledge they have learned in a simulated environment. They will assess and identify vulnerabilities, threats, and suspicious activity in information technology systems and networks; assess the implication of threats; and implement management and mitigation responses to protect and defend sensitive information and intellectual property. Prerequisite: BUS 350, CBD 330, 332, 334, CBD 336.

Student Learning Outcomes

Students will:

1. Identify and assess cyber threats.
2. Analyze the implications of threats.
3. Implement defensive strategies.

Course Topics

1. Foundations of Cyber Defense
2. Vulnerability Management
3. Simulated Network Environment
4. Reconnaissance and Data Collection
5. Vulnerability Scanning
6. Defense and Offensive Techniques

CBD 330 INTRODUCTION TO CYBER DEFENSE (3)

In this course, students learn the basic concepts, terminology, and technologies that comprise the field of cyber defense. Students in this course are introduced to topics such as risk/ threats in the cyber environment, threat assessment, cyber-defense terminology, cyber-defense planning, and general cyber-defense management.

Student Learning Outcomes

Students will:

1. Understand the fundamental concepts, terminology, and technologies of cyber defense.
2. Analyze and assess risks and threats in the cyber environment.
3. Develop foundational skills in planning and managing cyber defense systems.
4. Explore key elements of information security, including inspection, protection, and incident response.
5. Gain insight into legal, ethical, and professional issues in cybersecurity.

Course Topics

1. Foundations of Cyber Defense
2. The Need for Security
3. Legal, Ethical, and Professional Issues
4. Risk Management
5. Security Technologies
6. Cryptography
7. Physical Security
8. Implementing Information Se
9. Information Security Maintenance

CBD 332 CYBER DEFENSE NETWORKING (3)

Students in this course explore the fundamentals of network security and related topics. This course facilitates an understanding of the fundamentals of networking configurations and protocols, as well as threat and vulnerability recognition and mitigation from the perspective of the CIA triad: eavesdropping (confidentiality), man-in-the-middle (integrity), and denial-of-service (availability). Students will also engage in applied learning to reinforce lectures and provide practical implementation experience.

Student Learning Outcomes

Students will:

1. Evaluate key network risks and vulnerabilities.
2. Understand and apply security standards and models, including ISO and NIST frameworks.
3. Harden operating systems to defend against malware, network attacks, and other threats.
4. Deploy and manage network security measures, including firewalls and intrusion detection systems.
5. Protect data using encryption techniques, public/private key systems, and digital certificates.
6. Establish and enforce security policies to mitigate risks.
7. Prepare for post-incident investigations and manage responses to network breaches.

Course Topics

1. Network Defense Fundamentals
2. Risk Evaluation and Management
3. Security Technologies
4. Cryptography and Data Protection
5. Operating System Hardening
6. Security Policies and Standards
7. Incident Management

CBD 334 LEGAL AND ETHICAL ENVIRONMENT OF CYBER DEFENSE (W) (3)

In this course, students are exposed to the legal and ethical issues that relate to the field of cyber defense. In addition to learning about the laws and policies that shape and govern this field, students will also study topics such as General Data Protection Regulation (GDPR), the protection of information/ intellectual property, ethical hacking, and privacy concerns in public and private organization.

Student Learning Outcomes

Students will:

1. Understand the legal frameworks governing digital actions and cyber defense.
2. Analyze intellectual property laws and their implications in a digital age.
3. Explore U.S. and international privacy laws and their application in cyber defense.
4. Evaluate enterprise privacy concerns and strategies for compliance.
5. Gain hands-on knowledge of cyber defense team operations, including Blue, Red, and Purple Teams.

Course Topics

1. Cybersecurity Laws, Regulations, and Policies
2. Intellectual Property in the Digital Age
3. Privacy Laws and Regulations
4. Enterprise Privacy Concerns
5. Cyber Defense Team Operations
6. Ethical Hacking and Professional Responsibility

CBD 336 CYBER RISK MANAGEMENT AND MITIGATION (3)

This course explores cyber defense from a risk-management perspective. Students focus on strategies for assessing risk, as well as for implementing effective and proactive risk-management practices and risk-mitigation measures. Topics in this risk assessment include risk analysis, risk mitigation, risk management, networking components and Virtual Private Networks (VPN). Students will also learn about the resources and methods used for information assurance. The student will apply this knowledge to develop an assessment methodology and strategies for managing and mitigating risks in the cyber environment.

Student Learning Outcomes

Students will:

1. Understand the evolving cyber threat landscape and its impact on organizations.
2. Analyze and assess risks associated with cybersecurity using industry standards and methodologies.
3. Evaluate motivations of threat actors and types of vulnerabilities in systems.
4. Develop and implement effective cybersecurity controls and risk mitigation strategies.
5. Apply a risk-based approach to cybersecurity management.
6. Contrast and learn from high-profile data breaches to enhance risk management practices.

Course Topics

1. Digital Transformation and Cybersecurity
2. Data Breaches
3. Threat Actors and Events
4. Vulnerabilities
5. Cybersecurity Controls
6. Cyber Risk Management
7. Information Assurance Resources

CBD 451 PRACTICUM IN CYBER DEFENSE (3)

This is the capstone course for the major in cyber defense. This is an applied, lab-based class that provides students an opportunity to apply the knowledge they have learned in a simulated environment. They will assess and identify vulnerabilities, threats, and suspicious activity in information technology systems and networks; assess the implication of threats; and implement management and mitigation responses to protect and defend sensitive information and intellectual property. Prerequisite: BUS 350, CBD 330, 332, 334, CBD 336.

Student Learning Outcomes

Students will:

1. Identify and assess cyber threats.
2. Analyze the implications of threats.
3. Implement defensive strategies.

Course Topics

1. Foundations of Cyber Defense
2. Vulnerability Management
3. Simulated Network Environment
4. Reconnaissance and Data Collection
5. Vulnerability Scanning
6. Defense and Offensive Techniques