Cybersecurity (CYBR)

Courses

CYBR 3310 Introduction to Cybersecurity: 3 semester hours.
A survey course providing an introduction to the fields of Cybersecurity and Privacy. Emphasizes legal and ethical components of information security practices. The course is designed primarily for non-INFO majors. Not applicable toward INFO major. D

CYBR 3383 Security Design for Cyber-Physical Systems: 3 semester hours.
Examines frameworks and practices for designing safety, reliability and security into critical cyber-physical systems, emphasizing usability of these designs throughout the entire system lifecycle. PREREQ or COREQ: ESET 1181, ESET 2282, ESET 2223, ESET 2227 with a minimum grade of C-, or instructor approval. F, D

CYBR 3384 Risk Management for Cyber-Physical Systems: 3 semester hours.
Course covers assessment and management of risk for industrial cyber-physical systems, including asset identification, threat analysis, vulnerability analysis, consequence assessment, mitigation techniques, and general incident response. Lecture/Lab Course. PREREQ or COREQ: ESET 1181, ESET 2282, ESET 2223, ESET 2227, CYBR 3383 with a minimum grade of C-, or instructor approval. F, D

CYBR 4411 Intermediate Cybersecurity: 3 semester hours.
Focuses on homeland security, information assurance, integrity, control, and privacy. Covers CNSS-4011, NIST-800-16 standards, national policy, and international treaties. The course considers Software Deployment, Operations, Maintenance, and Disposal, including security issues around steady state operations and management of software, as well as security measures that must be taken when a product reaches its end of life. PREREQ: INFO 1150 or CYBR 3310, or permission of instructor. D

CYBR 4412 Systems Security for Senior Management: 1-3 semester hours.
Review of system architecture, system security measures, system operations policy, system security management plan, and provisions for system operator and end user training. COREQ: INFO 4419. PREREQ: CYBR 4416 or permission of instructor. D

CYBR 4413 Systems Security Administration: 1-3 semester hours.
Outlines the basic principles of systems security administration. The student will be introduced to the methods and technologies associated with running a system to maintain privacy and security. COREQ: INFO 4419. PREREQ: CYBR 4411 or permission of instructor. D

CYBR 4414 Systems Security Management: 1-3 semester hours.
Establishes a framework for managing both systems and systems administrators operating in a secure and private computing environment. The course deals with facilities management, contingency plans, laws, standards of conduct and operations management. COREQ: INFO 4419. PREREQ: CYBR 4413 or permission of instructor. D

CYBR 4415 System Certification: 1-3 semester hours.
Describes the techniques and methods for certifying a system is in compliance with national and governmental information assurance standards. Evaluates various certification methodologies. COREQ: INFO 4419. PREREQ: CYBR 4414 or permission of instructor. D

CYBR 4416 Risk Analysis: 1-3 semester hours.
Develops techniques to characterize and provide perspective on the likelihood of adverse events. Explains methods to characterize the consequences and general costs associated with the various adverse events occurring. The analysis provides insight into various likelihood and consequence combinations. COREQ: INFO 4419. PREREQ: CYBR 4415 or permission of instructor. D

CYBR 4417 Cybersecurity Engineer: 1-3 semester hours.
Focuses on the practical application of systems design and engineering principles and processes to develop secure systems. Topics include analysis of organizational needs, definition of security requirements, designing systems architectures, developing secure designs, implementing system security, and support of systems security assessment/authorization for organizations. PREREQ: CYBR 4411, CYBR 4413, CYBR 4414, CYBR 4415, CYBR 4416. D

CYBR 4419 Advanced Cybersecurity Practicum: 1-3 semester hours.
Significant cybersecurity experience including research coordinated by the faculty designed to provide broad exposure to issues in Information Assurance. Does not fulfill major/minor requirements. May be repeated for up to 6 credits. Graded S/U. PREREQ: Permission of instructor. D

CYBR 4471 Computer Forensics Essentials: 3 semester hours.
Introduction to issues of both in data privacy and computer forensics - using available tools, learners can reveal the stored passwords on their computer and access previously deleted data. Explains the role of computer forensics in both the business and private world, identifies the current techniques and tools for forensic examinations; describes and identifies basic principles of good professional practice for a forensic computing practitioner; develops familiarity with forensic tools and application in different situations. Risk exposure for electronic commerce businesses; offenders and abuses; criminal opportunities; evidential aspects, case studies, E-discovery, forensic readiness corporate planning and response, from evidence collection to business continuity; testing vulnerabilities; reverse engineering. Specific, evaluated graduate-level activities and/or performances are identified in the course syllabus. PREREQ: INFO 4407 and INFO 3380 or permission of instructor. D

CYBR 4472 Cloud Security Essentials: 1-3 semester hours.
Cloud computing provides for distributed computing and data storage capabilities. Instead of buying large servers to store data and being saddled with the cost of building and maintaining those systems, users can now purchase those servers from a third party with the ability to expand or contract those needs as necessary. This course will look at current research results in cloud security in order to identify opportunities for continued research in this field. PREREQ: INFO 4407 and INFO 3380 or permission of instructor. D

CYBR 4473 Continuous Monitor, Intrusion Analysis, Response: 1-3 semester hours.
Using principles continuous monitoring and baselines, develop knowledge and understanding of the strategies, techniques, and technologies used in attacking and defending networks and how to design secure networks and protect against intrusion, malware and other hacker exploits. Introduces methods of attacking and defending a network; design of secure information infrastructure; servers, networks, firewalls, workstations, and intrusion detection systems. Intrusion detection and network monitoring techniques; worms, viruses and other malware; operation, detection and response; principles of penetration testing for assessment of system security; hacker exploits, tools and countermeasures. Investigative techniques, ethical, legal and privacy issues. PREREQ: INFO 4407, CYBR 4411, and INFO 3380 or permission of instructor. D

CYBR 4474 SCADA Management and Lab: 1-3 semester hours.
Supervisory control and data acquisition systems are used to control many utility networks, chemical plants, pipelines and many other types of industries. This course will examine the vulnerabilities associated with these systems and discuss how they can be made secure from outside attack. Fundamentals of software-controlled processes will also be discussed. PREREQ: INFO 4411, INFO 4407, and INFO 3380 or permission of instructor. D

CYBR 4481 Defending Critical Infrastructure and Cyber Physical Systems: 3 semester hours.
Covers system of systems analysis and attack vector analysis as foundational frameworks to guide identification, selection and use of appropriate defensive techniques and technologies for critical infrastructure environments. Lecture/Lab. PREREQ: ESET 2282, CYBR 3383, CYBR 3384 with a minimum grade of C-, or instructor approval. S, D

CYBR 4484 Secure Software Lifecycle Development: 3 semester hours.
In today's interconnected world, security must be included within each phase of the software lifecycle. This course contains the largest, most comprehensive collection of best practices, policies, and procedures to ensure a security initiative across all phases of application development, regardless of methodology. PREREQ: INFO 4482. D

CYBR 4486 Network Security for Industrial Environments: 3 semester hours.
Networking security fundamentals and implementation in industrial environments focusing on hosts, firewalls, and switches. Students will gain knowledge and experience in segmentation, secure access, network and host monitoring, and incident response.. PREREQ: ESET 2282, CYBR 3383 with a minimum grade of C-, or instructor approval. S, D

CYBR 4487 Professional Development and Certification: 3 semester hours.
Covers theoretical knowledge and practical skills in preparation for international certification in cybersecurity. Emphasizes professional ethics. PREREQ: CYBR 3383. PREREQ or COREQ: CYBR 3384, CYBR 4486, CYBR 4481 with a minimum grade of C-. S, D

CYBR 4488 Cybersecurity Current Intelligence Practicum: 1-3 semester hours.
Students in this course adopt the role of analysts closely following and examining current cybersecurity events to publish intelligence products. Course covers practical elements of requirements, sources, analysis, writing, editing, and management of finished intelligence. PREREQ: Instructor approval. F, S

CYBR 4489 Capstone in Industrial Cybersecurity: 3 semester hours.
Professionally-oriented cybersecurity project, to synthesize knowledge and skills gained throughout the program. Develops lifelong professional learning strategies. Fosters professional communication proficiency. May be repeated once. PRE-OR-COREQ: CYBR 4486, CYBR 4481 with a minimum grade of C-. F, S

CYBR 4498 Special Topics in Cybersecurity: 1-8 semester hours.
This course covers special topics in cybersecurity. PREREQUISITE: Instructor approval.

CYBR 4499 Experimental Course: 1-6 semester hours.
The content of this course is not described in the catalog. Title and number of credits are announced in the Class Schedule. Experimental courses may be offered no more than three times with the same title and content. May be repeated.