CYBERSECURITY, BACHELOR OF SCIENCE

Bachelor of Science in Cybersecurity

Cybersecurity (CYBR) is an emerging, rapidly expanding science that addresses problems in the fundamental understanding of the design, development, implementation and lifecycle support of secure information systems. The need for secure information systems has become a paramount concern as the computer-enabled, internet-connected, digital-based global society of the 21st century continues to emerge. The lack of adequately secure information systems has been cited as one of the likely impediments to the emergence of the digital society.

Cyber Operations Track (Optional)

The University of Nebraska at Omaha's undergraduate Cybersecurity degree program is one of the few National Security Agency (NSA) certified National Centers of Academic Excellence in Cyber Operations (CAE-CO). As a result, UNO's College of Information Science and Technology (IS&T) is able to offer undergraduate students majoring in Cybersecurity the option to pursue a specialized Cyber Operations (CO) track and complete the requirements set out by the NSA's CAE-CO program. Students already enrolled in the Bachelor of Science in Cybersecurity degree program have very few additional requirements to meet in order to complete the Cyber Operations track.

Writing in the Discipline

All UNO students are required to take a writing-in-the-discipline course within their major. Cybersecurity degree students must take CIST 3000.

Student Groups

NULLify is UNO's student-led computer security group. Contact the group at unonullify@gmail.com.

Visit NULLify on Facebook at nullifyuno.

Degree Requirements

Bachelor of Science in Cybersecurity

A minimum of 120 credit hours is required for a Bachelor of Science degree in Cybersecurity (BSIA). Thirty of the last 36 hours must be University of Nebraska at Omaha courses. Registering for courses without having taken the stated prerequisites could result in administrative withdrawal.

To obtain a Bachelor of Science in Cybersecurity, a student must fulfill the University General Education, College, and Departmental requirements. Some courses may satisfy requirements in more than one area, but credit is awarded only once, thereby reducing the total number of credit hours for the degree to 120. (This total does not include prerequisites.)

Code	Title	Credits
46 hours of University General Education courses (16 hours of which can be satisfied by courses in the required areas below)		30
9 hours of College of IS&T Core courses		9
8 hours of Mathematics courses		8
21 hours of Computer Science Core courses		21
27 hours of Cybersecurity Core courses		27
18 hours of Cybersecurity Elective courses		18
7 hours of elective/prerequisite courses		7
Total Credits		**120**

Code	Title	Credits
Prerequisite / Free Electives		
Select one of the following:		3-4
CSCI 1200 & CSCI 1204	COMPUTER SCIENCE PRINCIPLES and COMPUTER SCIENCE PRINCIPLES LABORATORY [1]	
CIST 1300	INTRODUCTION TO WEB DEVELOPMENT	
College of IS&T Core Courses for CYBR Majors		
CIST 1400	INTRODUCTION TO COMPUTER SCIENCE I	3
CIST 2100	ORGANIZATIONS, APPLICATIONS AND TECHNOLOGY [2]	3
CIST 3110	INFORMATION TECHNOLOGY ETHICS [3]	3
Mathematics Courses		
MATH 1950	CALCULUS I [5]	5
MATH 2030	DISCRETE MATHEMATICS	3
or CSCI 2030	MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE	
Computer Science Core Courses		
CSCI 1620	INTRODUCTION TO COMPUTER SCIENCE II	3
CYBR 2250	LOW-LEVEL PROGRAMMING	3
CSCI 3320	DATA STRUCTURES	3
CSCI 3550	COMMUNICATION NETWORKS	3
CSCI 3710	INTRODUCTION TO DIGITAL DESIGN AND COMPUTER ORGANIZATION	3
CSCI 4350	COMPUTER ARCHITECTURE	3
CSCI 4500	OPERATING SYSTEMS	3
Cybersecurity Core Courses		
CYBR 1100	INTRODUCTION TO INFORMATION SECURITY [4]	3
CYBR 2600	SYSTEM ADMINISTRATION	3
CYBR/CIST 3600	INFORMATION SECURITY POLICY AND AWARENESS	3
CYBR 3570	CRYPTOGRAPHY	3
CYBR 4360	FOUNDATIONS OF CYBERSECURITY	3
CYBR/CSCI 4380	DIGITAL FORENSICS	3
CYBR 4450	HOST-BASED VULNERABILITY DISCOVERY	3
CYBR 4460	NETWORK-BASED VULNERABILITY DISCOVERY	3
CYBR 4580	CYBERSECURITY CAPSTONE	3
Cybersecurity Elective Courses		
Select 18 hours from the following:		18
CYBR Electives		
CYBR 2980/4980	SPECIAL TOPICS IN CYBERSECURITY	
CYBR 3450	NATURAL LANGUAGE PROCESSING	
CYBR 4390	MOBILE DEVICE FORENSICS	
CYBR 4430	QUANTUM COMPUTING AND CRYPTOGRAPHY	
CYBR 4440	INDUSTRIAL CONTROL SYSTEM SECURITY	
CIST/CYBR 4540	COMPUTER SECURITY MANAGEMENT	
CYBR 4950	INTERNSHIP IN CYBERSECURITY	
CYBR 4990	INDEPENDENT STUDY IN INFORMATION ASSURANCE	
CSCI Electives		
CSCI 3660	THEORY OF COMPUTATION (NSA Cyber Operations Track)	
CSCI 4220	PRINCIPLES OF PROGRAMMING LANGUAGES	
CSCI/MATH 4560	NUMBER THEORY & CRYPTOGRAPHY	

CSCI 4830	INTRODUCTION SOFTWARE ENGINEERING	
ISQA Electives		
ISQA 3310	MANAGING THE DATABASE ENVIRONMENT	
ISQA 3910	INTRODUCTION TO PROJECT MANAGEMENT	
ISQA 4380	DISTRIBUTED TECHNOLOGIES AND SYSTEMS	
PSCI Electives		
PSCI 4250	INTELLIGENCE AND NATIONAL SECURITY (NSA Cyber Operations Track)	
PSCI 4260	INTERNATIONAL LAW (NSA Cyber Operations Track)	
Total Credits		**86-87**

1 NOTE: CSCI 1200 and CSCI 1204 count toward the Natural and Physical Sciences requirement.

2 NOTE: CIST 2100 counts toward Social Science requirement.

3 NOTE: CIST 3110 counts toward Humanities requirement.

4 NOTE: CYBR 1100 counts toward Global Diversity requirement.

5 Note: MATH 1950 is required for this degree program. This course will also satisfy UNO's General Education Quantitative Literacy requirement. Students who do not place into MATH 1950 are responsible for prerequisite courses MATH 1220, MATH 1320, and MATH 1330.
MATH 1120/STEM 1120, MATH 1130, and STAT 1530 will not serve as prerequisites for MATH 1950. These courses will satisfy the General Education Quantitative Literacy requirement; however, they do not satisfy the Math requirement for the degree program. Students are highly encouraged to consult with their academic advisor before enrolling in a particular course.

Cyber Operations Track (Optional)

Students already enrolled in the Bachelor of Science in Cybersecurity degree have the following additional requirements to meet in order to complete the Cyber Operations track:

- PSCI 4250 Intelligence and National Security*
- PSCI 4260 International Law*
- CSCI 3660 Theory of Computation *
- CYBR 8410 Distributed Systems and Network Security**
- CYBR 8420 Software Assurance **
- CSCI 8620 Mobile Computing and Wireless Networking**
- CYBR 8480 Secure Mobile and Internet of Things Development**
- CYBR 8000 Center of Academic Excellence -Cyber Operations Completion Certificate**

*These courses also apply towards the Cybersecurity elective requirements.

**Graduate level courses required for Cyber Operations track. Graduate level courses can be taken with special permission.

Minor Offered

- Cybersecurity Minor (http://catalog.unomaha.edu/undergraduate/college-information-science-technology/school-interdisciplinary-informatics-si2/cybersecurity-minor/)

Freshman

Fall		**Credits**
ENGL 1150	ENGLISH COMPOSITION I	3
CYBR 1100	INTRODUCTION TO INFORMATION SECURITY	3
CIST 1400	INTRODUCTION TO COMPUTER SCIENCE I	3
MATH 1950	CALCULUS I [1]	5
	Credits	**14**
Spring		
ENGL 1160	ENGLISH COMPOSITION II	3
CSCI 1620	INTRODUCTION TO COMPUTER SCIENCE II	3
CSCI 2030	MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE	3
CMST 1110 or CMST 2120	PUBLIC SPEAKING FUNDS or ARGUMENTATION AND DEBATE	3
Social Sciences		3
	Credits	**15**

Sophomore

Fall		
CIST 2100	ORGANIZATIONS, APPLICATIONS AND TECHNOLOGY	3
CYBR 2250	LOW-LEVEL PROGRAMMING	3
CIST 3000	ADVANCED COMPOSITION FOR IS&T	3
Free Elective		3
Natural & Physical Sciences		3
	Credits	**15**
Spring		
CIST 3110	INFORMATION TECHNOLOGY ETHICS	3
CSCI 3320	DATA STRUCTURES	3
CSCI 3710	INTRODUCTION TO DIGITAL DESIGN AND COMPUTER ORGANIZATION	3
Social Sciences/US Diversity		3
Natural & Physical Sciences with Lab		4
	Credits	**16**

Junior

Fall		
CYBR 2600	SYSTEM ADMINISTRATION	3
CYBR 3600	INFORMATION SECURITY POLICY AND AWARENESS	3
CYBR 3570	CRYPTOGRAPHY	3
CSCI 3550	COMMUNICATION NETWORKS	3
Cybersecurity Elective		3
	Credits	**15**
Spring		
CSCI 4350	COMPUTER ARCHITECTURE	3
CYBR 4360	FOUNDATIONS OF CYBERSECURITY	3
CYBR 4450	HOST-BASED VULNERABILITY DISCOVERY	3
Cybersecurity Elective		3
Cybersecurity Elective		3
	Credits	**15**

Senior

Fall		
CYBR 4460	NETWORK-BASED VULNERABILITY DISCOVERY	3
CSCI 4500	OPERATING SYSTEMS	3
Cybersecurity Elective		3
Cybersecurity Elective		3
Humanities & Fine Arts		3
	Credits	**15**

Spring		
CYBR 4580	CYBERSECURITY CAPSTONE	3
CYBR 4380	DIGITAL FORENSICS	3
Cybersecurity Elective		3
Humanities & Fine Arts		3
Free Elective		3
	Credits	**15**
	Total Credits	**120**

[1] MATH 1950 - Satisfies General Education Quantitative Literacy requirement

Cybersecurity with Cyber Operations Track - Optional

Freshman		
Fall		**Credits**
ENGL 1150	ENGLISH COMPOSITION I	3
MATH 1950	CALCULUS I [1]	5
CYBR 1100	INTRODUCTION TO INFORMATION SECURITY	3
CIST 1400	INTRODUCTION TO COMPUTER SCIENCE I	3
	Credits	**14**
Spring		
ENGL 1160	ENGLISH COMPOSITION II	3
CSCI 1620	INTRODUCTION TO COMPUTER SCIENCE II	3
CSCI 2030	MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE	3
Natural & Physical Sciences		3
Social Sciences		3
	Credits	**15**
Summer		
CMST 1110 or CMST 2120	PUBLIC SPEAKING FUNDS or ARGUMENTATION AND DEBATE	3
Free Elective		3
	Credits	**6**
Sophomore		
Fall		
CIST 2100	ORGANIZATIONS, APPLICATIONS AND TECHNOLOGY	3
CYBR 2250	LOW-LEVEL PROGRAMMING	3
CIST 3000	ADVANCED COMPOSITION FOR IS&T	3
Natural & Physical Sciences with Lab		4
Free Elective		3
	Credits	**16**
Spring		
CIST 3110	INFORMATION TECHNOLOGY ETHICS	3
CSCI 3320	DATA STRUCTURES	3
CSCI 3710	INTRODUCTION TO DIGITAL DESIGN AND COMPUTER ORGANIZATION	3
Cybersecurity Elective		3
Social Sciences/US Diversity		3
	Credits	**15**
Summer		
Humanities & Fine Arts		3
Cybersecurity Elective		3
	Credits	**6**
Junior		
Fall		
CYBR 2600	SYSTEM ADMINISTRATION	3
CYBR 3600	INFORMATION SECURITY POLICY AND AWARENESS	3
CYBR 3570	CRYPTOGRAPHY	3
CSCI 3550	COMMUNICATION NETWORKS	3
PSCI 4250	INTELLIGENCE AND NATIONAL SECURITY	3
	Credits	**15**
Spring		
CSCI 3660	THEORY OF COMPUTATION	3
CSCI 4350	COMPUTER ARCHITECTURE	3
CYBR 4360	FOUNDATIONS OF CYBERSECURITY	3
CYBR 4450	HOST-BASED VULNERABILITY DISCOVERY	3
PSCI 4260	INTERNATIONAL LAW	3
	Credits	**15**
Summer		
CSCI 4500	OPERATING SYSTEMS	3
	Credits	**3**
Senior		
Fall		
CYBR 4380	DIGITAL FORENSICS	3
CYBR 4460	NETWORK-BASED VULNERABILITY DISCOVERY	3
Cybersecurity Elective		3
CYBR 8410	CRYPTOGRAPHY AND NETWORK SECURITY	3
CYBR 8420	SOFTWARE ASSURANCE	3
	Credits	**15**
Spring		
CYBR 4580	CYBERSECURITY CAPSTONE	3
CSCI 8620	MOBILE COMPUTING AND WIRELESS NETWORKS	3
CYBR 8480	SECURE MOBILE DEVELOPMENT	3
CYBR 8000	CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE	0
Humanities & Fine Arts		3
	Credits	**12**
	Total Credits	**132**

[1] MATH 1950 - Satisfies General Education Quantitative Literacy requirement

This roadmap is a suggested plan of study and does not replace meeting with an advisor. Please note that students may need to adjust the actual sequence of courses based on course availability. Please consult an advisor in your major program for further guidance.

This plan is not a contract and curriculum is subject to change.

Additional Information About this Plan:

University Degree Requirements: The minimum number of hours for a UNO undergraduate degree is 120 credit hours. Please review the requirements for your specific degree program to determine all requirements for the program. In order to graduate on time (four years for an undergraduate degree), you need to take 30 credit hours each year.

Placement Exams: For Math, English, and Foreign Languages, a placement exam may be required. More information on these exams can be found at https://www.unomaha.edu/enrollment-management/testing-center/placement-exams/information.php

Please note that transfer credit or placement exam scores may change a suggested plan of study.

CYBR 1100 INTRODUCTION TO INFORMATION SECURITY (3 credits)
This course emphasizes our current dependence on information technology and how its security in cyberspace (or lack thereof) is shaping the global landscape. Several historical and contemporary global events that have been influenced by the exploitation of information technology motivates topics on cyber crime, malware, intrusion detection, cryptography, among others, and how to secure one's own data and computer system. Several aspects of this course are geared towards developing an understanding of the "cyberspace" as a new medium that breaks all geographical boundaries, while highlighting noticeable influences on it from social, political, economic and cultural factors of a geographical region.
Distribution: Global Diversity General Education course

CYBR 2250 LOW-LEVEL PROGRAMMING (3 credits)
This course will teach the cybersecurity (CYBR) students low-level programming in the 'C' and assembly languages, and the interrelationship between these two programming paradigms. The student will learn the various control structures in 'C' and how they are implemented in machine code, memory allocation and management, and the basics of allocation classes such as static versus automatic variables. The students will also learn assembly language in the 'C' environment and will be able to write useful, functional, stand-alone assembly language programs with no help from external libraries.
Prerequisite(s)/Corequisite(s): CSCI 1620. Not open to non-degree graduate students.

CYBR 2600 SYSTEM ADMINISTRATION (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various computer management requirements using both Windows and Linux operating systems on both physical and virtual machines. Topics include installation, creating and maintaining file systems, user and group administration, backup and restore processes, network configuration, system services, virtualization, and security administration.
Prerequisite(s)/Corequisite(s): CIST 1400 or Instructor Permission

CYBR 2980 SPECIAL TOPICS IN CYBERSECURITY (1-3 credits)
The course provides a format for exploring subject areas in Cybersecurity and related fields for sophomore undergraduate students. Specific topics vary, in keeping with research interests of faculty and students. Examples include network configuration, network security, forensics, regulatory compliance, web services and applications, vulnerability assessments, cloud computing security, and other issues in Cybersecurity.
Prerequisite(s)/Corequisite(s): Instructor permission required. Not open to non-degree graduate students.

CYBR 3350 SECURITY ADMINISTRATION - LINUX (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the a Linux-based Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.
Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3370 SECURITY ADMINISTRATION - WINDOWS (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the Windows Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.
Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission

CYBR 3450 NATURAL LANGUAGE PROCESSING (3 credits)
The course will provide overview of the topics in natural language processing such as word and sentence tokenization, syntactic parsing, semantic role labeling, text classification. We will discuss fundamental algorithms and mathematical models for processing natural language, and how these can be used to solve practical problems. We will touch on such applications of natural language processing technology as information extraction and sentiment analysis. (Cross-listed with CSCI 3450).
Prerequisite(s)/Corequisite(s): Prereq: CSCI 2030 with C- or better; Co-req: CSCI 3320 with C- or better; Students should be comfortable w/ scripting (Python is the language extensively used in natural language processing tools including NLTK). Not open to non-degree graduate students.

CYBR 3570 CRYPTOGRAPHY (3 credits)
The course will provide a broad overview of the concepts, fundamental ideas, vocabulary, and literature base central to the study and development of cryptography and cryptanalysis. This course will explore historical development of cryptography, as well as methods used to defeat it.
In addition, the course will cover the mathematical foundations of cryptography today, as well as some current uses of such cryptography, such as public key infrastructures, the Internet Key Exchange protocol, and more.
Prerequisite(s)/Corequisite(s): CSCI 3320 or ISQA 3300. Not open to non-degree graduate students.

CYBR 3600 INFORMATION SECURITY, POLICY AND AWARENESS (3 credits)
This course will cover the planning and development for information governance, security policies and procedures, and security awareness. (Cross-listed with CIST 3600)
Prerequisite(s)/Corequisite(s): CIST 2100; CIST 3110, which may be taken concurrently.

CYBR 4000 CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.
Prerequisite(s)/Corequisite(s): Instructor Permission. The program committee will work w/ the UG advisors to verify that the student has fulfilled the requirements for this designation. If the student has fulfilled (or will soon) all the requirements, they may register for this class.

CYBR 4360 FOUNDATIONS OF CYBERSECURITY (3 credits)
Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 8366, CSCI 8366).
Prerequisite(s)/Corequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3400 OR By instructor permission

CYBR 4380 DIGITAL FORENSICS (3 credits)
Digital forensics involves the preservation, identification, extraction, analysis and documentation of digital evidence stored on a variety of electronic devices. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a forensics investigation. Topics include: an introduction to digital forensics, data acquisition, first response, memory forensics, operating system forensics, and network forensics. Students will be required to perform several forensics analyses in a controlled lab environment, including acquiring forensically sound hard drive images, memory images and analyzing these using industry standard tools, such as Forensic Toolkit (FTK). The Digital Forensics class is designed for Cybersecurity, Computer Science and other qualified students to learn what actions are both appropriate and required for preserving, collecting and analyzing digital evidence in cases of intrusion, data theft or other cybercrimes. (Cross-listed with CSCI 4380).
Prerequisite(s)/Corequisite(s): The student must take the following before enrolling: CYBR 3600 or CIST 3600, CSCI 3550 or ISQA 3400, CYBR 3370, CYBR 3350. Alternatively, instructor permission can be sought for students who have not met all of the above requirements.

CYBR 4390 MOBILE DEVICE FORENSICS (3 credits)
Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a mobile device forensics investigation. Topics include: an introduction to digital and mobile device forensics, mobile forensics standards, acquisition methods (manual, logical, physical and provider-side), Android and iOS filesystem analysis, decoding approaches, application data analysis, and report writing. Students will be required to perform several investigations in a controlled lab environment, including acquiring forensically sound evidence and analyzing these using industry standard tools. (Cross-listed with CYBR 8396).
Prerequisite(s)/Corequisite(s): CYBR 4380/8386 - Computer and Network Forensics or Instructors Permission

CYBR 4430 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)
The course builds an understanding of exciting concepts behind quantum computing and quantum cryptography. In doing so it will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms such as quantum Fourier transformation, Shor's algorithm and Grover's algorithm, quantum key exchange, quantum encryption, and secure quantum channels that are built using these principles. It will also discuss advantages of quantum computing and cryptography over classical computing and cryptography and limitations thereof. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course, students will also implement several of the quantum algorithms. (Cross-listed with CYBR 8436, CSCI 4430).
Prerequisite(s)/Corequisite(s): Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission.

CYBR 4440 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)
The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 8446)
Prerequisite(s)/Corequisite(s): CSCI 3550.

CYBR 4450 HOST-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various "packing" algorithms for computer viruses, the viruses themselves, operating system "hooking", "fuzzing", and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 8456.)
Prerequisite(s)/Corequisite(s): CSCI 3710 and CYBR 2250

CYBR 4460 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)
The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 8466)
Prerequisite(s)/Corequisite(s): CSCI 3550

CYBR 4540 COMPUTER SECURITY MANAGEMENT (3 credits)
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 8546, ISQA 8546)
Prerequisite(s)/Corequisite(s): IASC 4360 or permission of the instructor.

CYBR 4580 CERTIFICATION AND ACCREDITATION OF SECURE SYSTEMS (CAPSTONE) (3 credits)
This is the BSIA capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package.
Prerequisite(s)/Corequisite(s): CIST 3600 or CYBR 3600; CIST 4360; CYBR 3350 or CYBR 3370; and CIST 4540 or CYBR 4540 may be taken prior to or concurrently. Not open to non-degree graduate students.

CYBR 4950 INTERNSHIP IN CYBERSECURITY (1-3 credits)
The course provides a format for a student to work with a local or national industry partner in a cyber-security oriented position, and to receive credit for this practical experience. The internship may or may not be a paid position, but will definitely be directly related to the Cybersecurity degree program. The class is proposed and organized by the student, with participating faculty supervising and input provided by the industry partner.
Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 4980 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 8986)
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 4990 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics which are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.
Prerequisite(s)/Corequisite(s): Instructor Permission