Department of Mathematics and Computer Science

Associate Professors: Brooke M. Andersen, Kevin J. Carlin, Robert M. Fry, Suzanne Kelton; *Assistant Professors*: Joseph A. Alfano (Chairperson), Matthew Creek, William Katcher; *Visiting Instructor*: Suzanne L. Kozak; *Lecturers*: Ali Al-Faris, Paul Chase, Pawan Gupta, Dana James, Karen McGrail, Gerald Taylor, Keith Trott, Maria Cevallos Warren.

MAJOR IN CYBERSECURITY (14)

Cyberspace is a dynamic and evolving ecosystem, with complex, multifaceted networks that connect individuals, organizations and national and international entities. However, cyberspace's expansion presents new weaknesses to exploit, making it vulnerable to intrusion and exploitation. Cyber threats and vulnerabilities have grown exponentially with the explosion of technology and connectedness, affecting individuals, organizations, and nations alike. And while cyber threats and vulnerabilities challenge our economic prosperity, organizational sustainability and individual identity and privacy, they have also emerged as a leading threat to national security.

The Assumption College Bachelor of Science in Cybersecurity offers a technology-based education, using methods in computing and information science, engineering, social science and technology management that also foster innovation and entrepreneurship in the digital information economy. The faculty, drawn from different areas of expertise in cybersecurity, will engage students in finding solutions to emerging global cyber threats. At Assumption, a Bachelor of Science in Cybersecurity will educate the next generation of leaders and architects in cybersecurity, who possess technological expertise and practical training to help secure, develop, and sustain the cyberspace ecosystem.

LEARNING GOALS

Assumption College Cybersecurity program graduates will be able to:

- Apply knowledge of computing and information technologies and use software development and security analysis tools to produce effective designs and solutions for specific cybersecurity problems within a variety of computing platforms and employing an approved secure systems development process model;
- Identify, analyze, and synthesize scholarly and professional literature relating to the fields of cybersecurity, information security, or information assurance, to help solve specific problems and to stay abreast of the rapidly changing security context;
- Participate as an active and effective member of a project team engaged in achieving specific computer-based cybersecurity results or solutions;
- Communicate, both orally and in writing, and negotiate with colleagues and other stakeholders including employees, managers, and executives within and between organizations;
- Demonstrate sensitivity to and sound judgment on ethical issues as they arise in cybersecurity and will adhere to accepted norms of professional responsibility;
- Integrate their technical expertise with knowledge from other disciplines, such as computer science, data analytics, economics, management science, psychology and human factors, to arrive at practical cybersecurity solutions that are effective in real organizations; and
- Use appropriate tools to prevent, detect, respond, and recover from cyber-attacks.

The Bachelor of Science in Cybersecurity comprises 14 required courses: one course in Statistics; three courses in Computer Science; four Cybersecurity Core courses; and six advanced courses in Cybersecurity including an Independent Cybersecurity Project or Internship.

Required Courses (14)

First Year

ECO 115	Statistics, or PSY 224, or SOC 300
CSC 117	Introduction to Programming, or CSC 120 Statistical Programming

CYB 115 Cybersecurity Fundamentals

Sophomore Year

CSC 321 Database Management Systems
CSC/CYB 230 Networking and Data Communications
CSC/CYB 235 Securing Wired and Wireless Networks
CYB 265 Operating Systems Administration
CSC 303 Operating Systems

Junior Year

CYB 304 Cryptography
CYB 318 Software and Application Security
CYB 328 Computer, Network Forensics and Digital Investigations
CYB 401 Preparing for Cyber Disasters

Senior Year

CYB 338 Ethical Hacking
CYB 438 Independent Cybersecurity Project or Internship

Course Descriptions

CYBERSECURITY (CYB)

CYB 115 CYBERSECURITY FUNDAMENTALS

This course provides a bird's eye view of the evolving cyberspace ecosystem, the interoperability of physical and social networks, and methods and techniques in securing that ecosystem. Students will explore the ethical, legal, and technical aspects of cybercrime and methods of prevention, detection, response and recovery. The value of strong moral character, integrity, and trust as prized attributes of cybersecurity practitioners will be highlighted. Students will be introduced to essential cybersecurity topics including operating system models and mechanisms for mandatory and discretionary controls, data models, basic cryptography and its applications, security in computer networks and distributed systems, inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses, an overview of the information security planning and staffing functions, data mining and data science, and policy and assurance issues. The advantages and inherent value of being prepared as a life-long learner with a strong liberal-arts background will be emphasized with the opportunity for students to complete a service-learning project tailored to their academic/career goals. No prior computer programming experience is required. Basic competency in computer operation is required. (Fall, Spring)
Albert/*Three credits*

CSC/CYB 230 NETWORKING AND DATA COMMUNICATIONS

This course expands upon the principles and current trends in computer networks as identified in Cybersecurity Fundamentals. Students will deepen their understanding of wide area networks (WANs), local area networks (LANs) and their architectures across which data travels and communicates. Subjects will include the open systems interconnection (OSI) model, transmissions control protocol / internet protocol (TCP/IP), open systems, topologies and internet connected devices. Through in-class projects, theoretical and practical approaches toward building and maintaining local area networks will be covered.
Prerequisites: CYB 115 or CSC 117 or CSC 120, or Instructor's permission. (Fall)
Gupta/*Three credits*

CSC/CYB 235 SECURING WIRED AND WIRELESS NETWORKS

This course provides students who have a basic understanding of computer networking and data communications with the methods and techniques used to secure networks. Students will be required to design and build a secure local area network, incorporating all elements of the seven layers of the OSI Model. Students will learn the capabilities, limitations and vulnerabilities of a cyber network that can be dynamic yet strong against aggressive hackers and virus outbreaks. Also the goal of this course is to provide students with both technical and theoretical approaches to the deployment, securing and defending of wireless networks. Topics will address network attacks, intrusion detection, malware, rogue wireless networks and wireless networking

through the cloud. Students must already possess a basic knowledge of information security and networks. Team projects and presentations are required for completion. Prerequisites: CYB 115 and CSC/CYB 230, or Instructor's permission. (Spring)
Gupta/*Three credits*

CYB 265 OPERATING SYSTEMS ADMINISTRATION
Learn how best to protect computers, the data they store, process and transmit, and the users who use them, from a wide array of cybersecurity threats. This course will introduce students to operating systems administration within the context of cybersecurity. Students will learn how best to perform basic system administration operations with an emphasis on methods (e.g., managing applications, services, and network ports) to fortify the security of the computer's operating system. The class will provide coverage of methods used in the Microsoft Windows® and Linux® operating systems. Prerequisites: CYB 115, or Instructor's permission. (Fall 2020, Fall 2022)
Albert/*Three credits*

CYB 304 CRYPTOGRAPHY
Cryptography is a key component in securing data while it is stored, processed, transmitted, as well as web, computer application, and network communications. This course will introduce students to the principles of number theory and the practice of network security and cryptographic algorithms, including hash functions, symmetric and asymmetric cryptography and their common as well as their susceptibility to attacks/failures. Students will learn how best to compare, select and apply cryptographic approaches to fortify cybersecurity. Other topics include cryptographic algorithms and programming. Prerequisites: CYB 235, or Instructor's permission. (Spring 2022, Spring 2024)
Albert/*Three credits*

CYB 318 SOFTWARE AND APPLICATION SECURITY
Software security represents a key aspect in the field of cybersecurity. This course will ground students in the concepts of malware, malware analysis and preventive measures during software development that can mitigate malicious activity. Theoretical approaches to software security will be complemented by practical scenarios from which students can conduct future software design and investigations. Prerequisites: CYB 235, or Instructor's permission. (Fall 2021, Fall 2023)
Albert/*Three credits*

CYB 328 COMPUTER, NETWORK FORENSICS AND DIGITAL INVESTIGATIONS
This course studies the technology and practice of investigating the abuse of computing systems and digital devices. As criminal and adversarial activity becomes faster and less visible over networks, students must understand how to search for, and extract information from, cyberspace. This course will provide unparalleled insight into digital forensics methods and laws, complemented with practical lab work. This course also introduces students to the theory and practice of network traffic analysis and intrusion detection. Students will learn "traceback" techniques and information retrieval methods to identify different attacks. Topics covered will include network forensics, intrusion detection and response, case studies, and issues of cyber law and ethics. Students must have basic knowledge of networking, and operating systems. Team projects and presentations are required for completion. Prerequisites: CYB 235, or Instructor's permission. (Fall 2021, Fall 2023)
Albert/*Three credits*

CYB 338 ETHICAL HACKING
This course will introduce students to ethical hacking and penetration testing methods, learning to think like a cyber-criminal and develop secure countermeasures. Students will learn the systematic approaches to planning, reconnaissance, vulnerability identification and exploitation methods used by hackers around the world to compromise the security of existing networks, systems and applications. A variety of penetration-testing tools and techniques will be explored through hands-on activities. Identification of corresponding cybersecurity control recommendations will be highlighted. Prerequisites: CYB 235, or Instructor's permission. (Fall 2022, Fall 2024)
Albert/*Three credits*

CYB 401 PREPARING FOR CYBER DISASTERS
This course will provide students a full picture of securing a firm from a cyberattack. Topics will include preparatory measures that continuously investigate network integrity, data security, and backup archives. Students will also develop Cyber Disaster Response Plans that consider the legal, economic, and physical requirements needed to recover from a cyberattack. Prerequisites: CYB 235, or Instructor's permission. (Spring 2022, Spring 2024)
Albert/*Three credits*

CYB 438 INDEPENDENT CYBERSECURITY PROJECT OR INTERNSHIP

Students in the Cybersecurity program will have the option during one semester to conduct and present an independent cybersecurity project or intern part time with a cybersecurity employer in the business, government or nonprofit sectors. Prerequisites: Junior or Senior standing in Cybersecurity major, or Instructor's permission. (Fall, Spring)

Albert/*Three credits*