CYBERSECURITY

Program Overview

Just as computing technology has become an integral part of many aspects of our lives, the need to secure the operation of that technology has become critical. The importance of secure computational operations has had significant impacts in social, commercial, financial, industrial, and political realms, and will continue to grow as the right to privacy is tested.

In NJ and the surrounding Philadelphia and New York metro areas the demand is even greater, with over 27,000 unfilled cybersecurity positions. On a national level, cybersecurity has been recognized as a critical component of Homeland Security, and the Senate Appropriations committee funded cybersecurity efforts above the President's request for FY 2019. Students pursuing a B.S. in Cybersecurity will bring a powerful combination of a traditional liberal arts education with foundational knowledge and technical training needed to excel in the cybersecurity field. A Minor in Cybersecurity is also available.

Curriculum Overview

Rider students in this program will benefit from a curriculum aligned with the latest national guidelines, adaptable to meet the evolving demands of industry and research. Cybersecurity is a nascent academic affair, although it has been in existence for nearly as long as computers. Thus, any cybersecurity curriculum should be founded in basic principles: that the computers, including data, software, systems, and networks, as well as the people and organizations using the machines, are kept secure and operational. The courses comprising the major are foundational, with the concentrations offering breadth and expertise in a given aspect of cybersecurity.

Student Learning Outcomes

Graduates of the Cybersecurity major will be able to:

1. Graduate with a broad understanding of the nature of cybercrime and cybersecurity.
2. Graduate with a deep understanding of security at multiple levels.
3. Graduate with the ability to collaborate and apply their knowledge to real-world problems.
4. Graduate with a passion for lifelong learning, professional responsibility to uphold ethical behavior.

Degrees Offered:

- B.S. in Cybersecurity
- Minor in Cybersecurity

Contact

John Bochanski, Ph.D.
Associate Professor and Chairperson
Department of Computer Science and Physics
School of Science, Technology and Mathematics
Hennessy Science and Technology Center 204B
609-896-5184
jbochanski@rider.edu

Program Website: Cybersecurity (https://www.rider.edu/academics/colleges-schools/college-arts-sciences/science-technology-math/undergraduate/cybersecurity/)
Associated Department: Department of Computer Science and Physics (https://www.rider.edu/academics/colleges-schools/college-arts-sciences/science-technology-math/faculty-departments/computer-science-physics/)

Related programs:

- Computer Science (http://catalog.rider.edu/undergraduate/colleges-schools/arts-sciences/majors-minors-certificates/computer-science/)
- Criminal Justice (http://catalog.rider.edu/undergraduate/colleges-schools/arts-sciences/majors-minors-certificates/criminal-justice/)
- Homeland Security Policy (http://catalog.rider.edu/undergraduate/colleges-schools/arts-sciences/majors-minors-certificates/homeland-security/)

Cybersecurity Program Requirements

(57 credits)

Students must select either the Technical Track or the Policy Track.
Notes:

- Majors must complete either MTH 105 or MTH 210 to fulfill their mathematics core requirement.
- A grade of 'C' or better is required in all 100-level CSC or CYB courses.

Code	Title	Credits
Required Cybersecurity Core Courses:		**12**
CYB 105	Introduction to Cybersecurity	
CYB 110	Cybercrime and Cyberterrorism	
CYB 130	IT Fundamentals	
CSC 150	Cyber Ethics and Societal Impact	
Select either the Technical Track or the Policy Track		**36**
Technical Track:		
Complete the following required courses:		
CSC 110	Computer Science I	
CSC 120	Computer Science II	
CSC 130	Data Structures and Algorithms	
CSC 140	Discrete Structures	
CYB 200	Operating Systems & Cybersecurity	
CYB 240	Ethical Hacking and Penetration Testing	
CSC 250	Software Security Engineering	
CYB 260	Network Defenses and Countermeasures	
CSC 260	Computer Networks	
CYB 300	Developing & Deploying Cybersecurity Programs	
CYB 320	Cyber Forensics	
CSC 340	Cybersecurity Essentials	
Elective Courses		
Select two of the following Policy courses:		**6**
HLS 203/POL 203	Homeland Security	
HLS 204/POL 204	Development and Structure of the US Intelligence Community	
SOC 210	Criminal Investigation	

LAW 310	Cyberspace Law and Policy	
HLS 320	Defense Policy and Analysis	
HLS 331	Critical Infrastructure	
POL 351/HLS 351	Critical Views of Global Security	
Select one of the following Technical courses: [1]		**3**
CSC 320	Human-Computer Interaction	
CSC 350	Analysis of Algorithms	
CSC 380	Parallel and Distributed Systems	
Policy Track (36 credits)		
Complete the following required courses:		
SOC 150	Introduction to Forensics	
HLS 203/POL 203	Homeland Security	
HLS 204/POL 204	Development and Structure of the US Intelligence Community	
SOC 210	Criminal Investigation	
SOC 119	Introduction to Criminal Justice: Police, Courts, Corrections	
POL 301	Civil Liberties in the U.S.	
HLS 205	Spies, Double Agents, and Moles: The World of Counterintelligence	
or HLS 304/ POL 304	Political Behavior: Fear, Risk and Crisis	
HLS 220/POL 220	Terrorism & Counter Terrorism	
or HLS 322	Countering Domestic Extremism in the United States	
LAW 310	Cyberspace Law and Policy	
POL 327	Contemporary Issues in American Public Policy	
or HLS 320	Defense Policy and Analysis	
SOC 343	Policing and Counter Terrorism	
or HLS 332	Disaster Management and Incident Response	
POL 351/HLS 351	Critical Views of Global Security	
or HLS 331	Critical Infrastructure	
Elective Courses		
Select two of the following Technical courses (6 credits): [1]		
CSC 105	Fundamentals of Computer Science	
CSC 110	Computer Science I	
CSC 120	Computer Science II	
CSC 140	Discrete Structures	
CYB 200	Operating Systems & Cybersecurity	
CYB 240	Ethical Hacking and Penetration Testing	
CYB 320	Cyber Forensics	
Select one of the following Policy courses (3 credits):		
HLS 341	Cybersecurity Policy: Hacktivism and Cyberviolence	
HLS 334	Cyber Strategy	
Electives for either Track		
CYB 490	Cybersecurity Independent Study and Research	
CSC 491	Internship in Computer Science	
Total Credits		**57**

NOTE: Cybersecurity majors must also complete either MTH 105 or MTH 210 to fulfill their mathematics core requirement.

[1] Other technical electives are available for Cybersecurity B.S. undergraduates pursuing the **4+1 M.S.**:

- CYBR 500 Beyond Code: Cybersecurity in Context
- CYBR 510 Cryptogragphy for Cybersecurity
- CYBR 520 Managing Cyber Risks
- CYBR 530 Mobile Computing & Wireless Security

Cybersecurity Minor Requirements

(21 credits)

Code	Title	Credits
Required Courses		**12**
CYB 105	Introduction to Cybersecurity	
CYB 110	Cybercrime and Cyberterrorism	
CSC 150	Cyber Ethics and Societal Impact	
CYB 130	IT Fundamentals	
Select at least three of the following courses:		**9**
CSC 105	Fundamentals of Computer Science	
CSC 110	Computer Science I	
CSC 120	Computer Science II	
CSC 130	Data Structures and Algorithms	
CYB 200	Operating Systems & Cybersecurity	
CYB 240	Ethical Hacking and Penetration Testing	
CYB 260	Network Defenses and Countermeasures	
CYB 300	Developing & Deploying Cybersecurity Programs	
CYB 320	Cyber Forensics	
CSC 340	Cybersecurity Essentials	
CSC 260	Computer Networks	
CIS 319	Computer Forensics	
Total Credits		**21**

Academic Plan of Study

The following educational plan is provided as a sample only. Rider students who do not declare a major during their freshman year; who are in a Continuing Education Program; who change their major; or who transfer to Rider may follow a different plan to ensure a timely graduation. Each student, with guidance from their academic advisor, will develop a personalized educational plan.

Technical Track (p. 2)
Policy Track (p. 3)

Cybersecurity Technical Track

Course	Title	Credits
Year 1		
Fall Semester		
CYB 105	Introduction to Cybersecurity	3
CSC 110	Computer Science I	3

MTH 105 or MTH 210	Algebra and Trigonometry or Calculus I	4
CMP 120	Seminar in Writing and Rhetoric	3
HIS 150	Pre-Modern World: Evolution to Revolution	3
	Semester Credit Hours	**16**
Spring Semester		
CYB 110	Cybercrime and Cyberterrorism	3
CSC 120	Computer Science II	3
CSC 150	Cyber Ethics and Societal Impact	3
CMP 125	Seminar in Writing and Research	3
HIS 151 or HIS 152 or HIS 153	World in the Modern Era: Exploration to Globalization or Contemporary World: Historical Perspectives or Cold War: A Global History	3
	Semester Credit Hours	**15**
Year 2		
Fall Semester		
CYB 130	IT Fundamentals	3
CSC 140	Discrete Structures	3
Cybersecurity Policy Elective		3
Social Perspectives Course		3
Aesthetic Perspectives: Literature		3
	Semester Credit Hours	**15**
Spring Semester		
CYB 200	Operating Systems & Cybersecurity	3
CSC 260	Computer Networks	3
Social Perspectives Course		3
Two Elective Courses [1]		6
	Semester Credit Hours	**15**
Year 3		
Fall Semester		
CYB 240	Ethical Hacking and Penetration Testing	3
CYB 260	Network Defenses and Countermeasures	3
CSC 130	Data Structures and Algorithms	3
Foreign Language 1 of 2		3
Philosophical Perspectives Course		3
	Semester Credit Hours	**15**
Spring Semester		
CSC 250	Software Security Engineering	3
CSC 340	Cybersecurity Essentials	3
Cybersecurity Policy Elective		3
Foreign Language 2 of 2		3
Aesthetic Perspectives: Fine Arts		3
	Semester Credit Hours	**15**
Year 4		
Fall Semester		
CYB 300	Developing & Deploying Cybersecurity Programs	3
Cybersecurity Technical Elective		3
Elective Credits [1]		8
	Semester Credit Hours	**14**
Spring Semester		
CSC 350	Analysis of Algorithms	3
Four Elective Courses [1]		12
	Semester Credit Hours	**15**
	Total Credit Hours for Graduation	**120**

[1] Please note that elective credits may be used to complete requirements in a second major or a minor.

Cybersecurity Policy Track

Course	Title	Credits
Year 1		
Fall Semester		
CYB 105	Introduction to Cybersecurity	3
CSC 110	Computer Science I	3
MTH 105 or MTH 210	Algebra and Trigonometry or Calculus I	4
CMP 120	Seminar in Writing and Rhetoric	3
HIS 150	Pre-Modern World: Evolution to Revolution	3
	Semester Credit Hours	**16**
Spring Semester		
CYB 110	Cybercrime and Cyberterrorism	3
CSC 150	Cyber Ethics and Societal Impact	3
SOC 150	Introduction to Forensics	3
CMP 125	Seminar in Writing and Research	3
HIS 151 or HIS 152 or HIS 153	World in the Modern Era: Exploration to Globalization or Contemporary World: Historical Perspectives or Cold War: A Global History	3
	Semester Credit Hours	**15**
Year 2		
Fall Semester		
SOC 119	Introduction to Criminal Justice: Police, Courts, Corrections	3
HLS 203	Homeland Security	3
Cybersecurity Technical Elective		3
Social Perspectives Course		3
Aesthetic Perspectives: Literature		3
	Semester Credit Hours	**15**
Spring Semester		
HLS 204	Development and Structure of the US Intelligence Community	3
SOC 210	Criminal Investigation	3
Social Perspectives Course		3
Two Elective Courses [1]		6
	Semester Credit Hours	**15**
Year 3		
Fall Semester		
POL 301	Civil Liberties in the U.S.	3

HLS 304	Political Behavior: Fear, Risk and Crisis	3
or HLS 205	or Spies, Double Agents, and Moles: The World of Counterintelligence	
Foreign Language 1 of 2		3
Philosophical Perspectives Course		3
Elective Course [1]		3
	Semester Credit Hours	**15**
Spring Semester		
HLS 220	Terrorism & Counter Terrorism	3
LAW 310	Cyberspace Law and Policy	3
Cybersecurity Technical Elective		3
Foreign Language 2 0f 2		3
Aesthetic Perspectives: Fine Arts		3
	Semester Credit Hours	**15**
Year 4		
Fall Semester		
POL 327	Contemporary Issues in American Public Policy	3
Cybersecurity Policy Elective		3
Three Elective Courses [1]		9
	Semester Credit Hours	**15**
Spring Semester		
SOC 343	Policing and Counter Terrorism	3
POL 351	Critical Views of Global Security	3
Elective Credits [1]		8
	Semester Credit Hours	**14**
	Total Credit Hours for Graduation	**120**

[1] Please note that elective credits may be used to complete requirements in a second major or a minor.

Courses and Descriptions

CYB 105 Introduction to Cybersecurity 3 Credits
Introduction to Cybersecurity introduces students to this interdisciplinary field by exploring the technology, policies, and processes that enable assured computer operations. Students will be introduced to recent developments in cybercrime such as phishing, ransomware, viruses, and worms. Students will also learn about the policy and legislation regarding privacy, terrorism, hacktivism, and the dark web. Students will also be introduced to programming and networking concepts.

CYB 110 Cybercrime and Cyberterrorism 3 Credits
This course explores the world of cybercrime and cyber terrorism. Students will learn about the social and legal aspects of cybercrime and the technical tools that enable the investigation of these acts. They will discuss and review several definitions and types of cybercrime, and the roles of private sectors and law enforcement in detecting, investigating and preventing these acts.

CYB 130 IT Fundamentals 3 Credits
IT Fundamentals is designed to immerse students in the essentials of computer hardware and software. The IT Fundamentals course provides students with principles of data and technology that frame and define cybersecurity and insight into the importance of cybersecurity and the integral role of cybersecurity professionals. Students will explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

CYB 200 Operating Systems & Cybersecurity 3 Credits
This course focuses on the fundamental properties of three major operating systems (Linux, MacOS, and Windows). The course covers file systems, command line interfaces, and shell scripting. Students will learn how to manage user groups while focusing on security. They will also be introduced to SQL database architecture.
Prerequisite(s): CYB 130.

CYB 240 Ethical Hacking and Penetration Testing 3 Credits
This course introduces students to the methods of penetration testing and hacking as method of locating and successfully exploiting computer systems for the purpose of making computer systems more secure. This process includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real and generating specific and effective recommendations for addressing and fixing security issues discovered vulnerability assessments and penetration.
Prerequisite(s): (CYB 200 with a minimum grade of D or CSC 240 with a minimum grade of D) and CSC 260 with a minimum grade of D.

CYB 260 Network Defenses and Countermeasures 3 Credits
This course in network defenses and countermeasures prepares students to defend networks against attacks by implementing proactive protection measures and by responding to active and potential threats. It covers multiple techniques for network defense, including firewalls, intrusion-detection systems, VPNs, encryption, and system hardening.
Prerequisite(s): CYB 240.

CYB 300 Developing & Deploying Cybersecurity Programs 3 Credits
In Developing and Deploying Cybersecurity Programs, students will learn how to create cybersecurity policies, standards, guidelines and plans, and the differences between them. Students will learn how threats develop, and how threat actors launch attacks on their targets. The material in this course conforms to the NIST Cybersecurity Framework and the ISO/IEC 27000-series standards.
Prerequisite(s): CSC 260 with a minimum grade of D.

CYB 320 Cyber Forensics 3 Credits
This course covers the technical and legal aspects of cyber forensics, including general forensic procedures, electronic discovery, imaging, hashing, file recovery, mismatched file types, and preserving the chain of evidence. Students will perform detailed cyber forensic analyses on compromised system images, using both open-source and court-approved digital forensic software tools to conduct forensic examinations, write analytical reports, and practice mock courtroom presentations.
Prerequisite(s): CYB 200.

CYB 490 Cybersecurity Independent Study and Research 3 Credits
Immerses the student in guided research. The student learns to organize material, use the literature, obtain reproducible data, and synthesize the results of the study. If possible, the student will publish the results or present them at a scientific meeting.

CYB 491 Internship in Cybersecurity 1-4 Credits
A supervised research experience in an approved organization where qualified students gain real-world knowledge and utilize their academic training in a professional environment. Placement may be in private, public, non-profit, or governmental organizations under the guidance of a mentor. The mentor and student will have regular consultation with the departmental internship coordinator to assess the student's progress. Normally, 40 hours of internship per credit is required. The grade for the course will be determined by the student's overall performance in their research work, a research paper documenting their work with their internship mentor and an oral or poster presentation at the end of the semester. Available for juniors and seniors.
Prerequisite(s): 2.5 GPA and Permission of Dept. Chair/Program Director.