Cybersecurity combines essential computer science with conceptual and practical specialization in security to prepare students for hands on, deeply technical work in the field. The ability to frame problems, select computational models, design program structures, and develop efficient algorithms is as important in computer science as software implementation skill. All cybersecurity students take the standard computer science course sequence, covering content such as basic programming, object-oriented design, computer architecture and operating systems, computer networks and distributed systems, and algorithmic complexity and computability theory. These courses lay the foundation for cybersecurity-specific course work.

Cybersecurity course work covers key areas in the field, from a broad overview of the topical space (including threat modeling, symmetric and asymmetric key cryptography, authentication, access control, social engineering, simple exploits, basic systems security, malware, the cybercrime underground, and advanced persistent threat actors) to deep dives into the design of secure operation systems and applications. Fundamental topics include analyzing prevalent classes of attacks against systems, security vulnerabilities and defense techniques, limitation of damage and strategic recovery, design and implementation of distributed authentication protocols, and existing standardized security protocols and legal infrastructure relating to privacy, data ethics, data security, hacking, automation, and intellectual property. In addition, cybersecurity students have access to a wide array of electives, including courses on wireless networking, software vulnerabilities, cybersecurity risk management and assessment, digital forensics, and criminology.

Programs

Bachelor of Science (BS)

- Cybersecurity (http://catalog.northeastern.edu/undergraduate/computer-information-science/cybersecurity/cybersecurity-bs)

Courses

Search CY Courses using FocusSearch (http://catalog.northeastern.edu/course-search/?subject=CY)

CY 2550. Foundations of Cybersecurity. 4 Hours.

Presents an overview of basic principles and security concepts related to information systems, including workstation security, system security, and communications security. Discusses legal, ethical, and human factors and professional issues associated with cybersecurity, including the ability to differentiate between laws and ethics. Offers students an opportunity to use a substantial variety of existing software tools to probe both computer systems and networks in order to learn how these systems function, how data moves within these systems, and how these systems might be vulnerable. Covers security methods, controls, procedures, economics of cybercrime, criminal procedure, and forensics.

CY 2991. Research in Cybersecurity. 1-4 Hours.

Offers an opportunity to conduct introductory-level research or creative endeavors under faculty supervision.

CY 3740. Systems Security. 4 Hours.

Introduces the fundamental principles of designing and implementing secure programs and systems. Presents and analyzes prevalent classes of attacks against systems. Discusses techniques for identifying the presence of vulnerabilities in system design and implementation, preventing the introduction of or successful completion of attacks, limiting the damage incurred by attacks, and strategies for recovering from system compromises. Offers opportunities for hands-on practice of real-world attack and defense in several domains, including systems administration, the Web, and mobile devices. Presents the ethical considerations of security research and practice.

CY 4170. The Law, Ethics, and Policy of Data and Digital Technologies. 4 Hours.

Describes the legal and ethical issues associated with collection, use, disclosure, and protection of digital information. Emphasizes legal infrastructure relating to privacy, data ethics, data security, hacking, automation, and intellectual property. Articulates the basic set of rules and rights that are relevant to data practices and protection, evaluates how these rules apply in context, and critically analyzes their efficacy and social impact.

CY 4740. Network Security. 4 Hours.

Studies topics related to Internet architecture and cryptographic schemes in the context of security. Provides advanced coverage of the major Internet protocols including IP and DNS. Examines denial of service, viruses, and worms, and discusses techniques for protection. Covers cryptographic paradigms and algorithms such as RSA and Diffie-Hellman in sufficient mathematical detail. The advanced topics address the design and implementation of authentication protocols and existing standardized security protocols. Explores the security of commonly used applications like the Web and e-mail.

CY 4770. Cryptography. 4 Hours.

Studies the design of cryptographic schemes that enable secure communication and computation. Emphasizes cryptography as a mathematically rigorous discipline with precise definitions, theorems, and proofs and highlights deep connections to information theory, computational complexity, and number theory. Topics include pseudorandomness; symmetric-key cryptosystems and block ciphers such as AES; hash functions; public-key cryptosystems, including ones based on factoring and discrete logarithms; signature schemes; secure multiparty computation and applications such as auctions and voting; and zero-knowledge proofs.

CY 4930. Cybersecurity Capstone. 4 Hours.

Provides the culmination of the learned principles and methodologies for identifying and addressing cybersecurity issues in organizations. Offers students an opportunity to work in small groups to identify and scope a current cybersecurity problem/challenge. Requires students to submit a written proposal about the project, complete with motivation, literature research, and reasons for the study; create a work plan to develop a solution to include the development and identification of the data necessary to properly solve the problem/challenge; and create a final report.
CY 4940. Research Projects on National Security. 4 Hours.
Engages students in national cybersecurity/information systems security problems. Offers students an opportunity to learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results. Working in small groups under the mentorship of external mentors from government and industry, each student has an opportunity to formulate, carry out, and present original research on current cybersecurity/information assurance problems of interest to the nation. As part of this research, students are required to submit a written proposal about the project, complete with motivation, literature research, and reasons for the study; create a work plan for the research problem; and create a final report.

CY 5001. Cyberspace Technology and Applications. 3 Hours.
Covers primary technologies and skills needed to develop Windows and Linux systems administration. Orient techniques and tools to serve as instruments of security administrators and cybersecurity professionals. Offers students an opportunity to train in the administration of operating systems, computer communications, and scripting through the use of practical hands-on labs running on virtual machines hosted in cloud computing environments. Also provides an overview of virtualization technologies and cloud computing models.

CY 5002. Concrete Mathematics. 3 Hours.
Offers students an opportunity to obtain a systematic understanding of mathematics necessary for mastering cyberspace tools and methods. Seeks to train students in mathematical concepts and the pragmatic use of these concepts in the field of information assurance and cybersecurity. Covers theory and hands-on exercises. Combines lectures with computer-based examples and assignments. Students not in the information assurance ALIGN program may require instructor approval for enrollment.

CY 5004. Introduction to Cyberspace Programming 1. 3 Hours.
Offers students an opportunity to obtain a systematic understanding of cyberspace programming languages and methods. Seeks to train students in Python using command-line interface-based editors and compilers, as well as integrated development environments, with industry-standard operating systems running on virtual machines. Trains students by implementing programming principles and methods, spanning the evolution of computer systems. Combines lectures with multiple computer-based exercises. Students not in the information assurance ALIGN program may require instructor approval for enrollment.

CY 5010. Foundations of Information Assurance. 4 Hours.
Presents an overview of basic principles and security concepts related to information systems, including operating system security, communications and network security, and software security. Introduces information security via concepts of confidentiality, integrity, and availability. Discusses ethical, legal, and privacy ramifications while reviewing various laws such as the Patriot Act, GLBA, and Global Data Privacy regulation. Covers security methods, controls, procedures, economics of cybercrime, criminal procedure, and forensics. Describes the use of cryptography as a tool, software development processes, and protection. Seeks to build a common cross-disciplinary understanding in the foundations of information assurance and cybersecurity.

CY 5040. Introduction to Cyberspace Programming 2. 4 Hours.
Offers students an opportunity to obtain a systematic understanding of cyberspace programming languages and methods. Trains students in Python, C, and assembly languages using command-line interface-based editors and compilers; integrated development environments, with industry-standard operating systems running on virtual machines; and the implementation of programming principles and methods spanning the evolution of computer systems.

CY 5061. Cloud Security. 2 Hours.
Introduces the fundamentals of cloud computing while segueing into understanding its various security challenges, threat models, and data privacy issues in regard to compliance and legal decisions. Examines the strategies to implement security controls, perform risk assessments, handle incident detection and response, while emphasizing maintaining a business-minded security life cycle for cloud-based environments.

CY 5062. Introduction to IoT Security. 2 Hours.
Aims to provide a foundation for understanding the main issues associated with information security in a widely connected world in the context of Internet of Things (IoT). Emphasizes the vulnerabilities and threats of the IoT-based systems. Offers students an opportunity to learn the essentials of the IoT technologies and the underlying mechanisms for protecting information.

CY 5120. Applied Cryptography. 4 Hours.
Surveys the principles and the practices of cryptography. Overviews the core cryptographic algorithms: symmetric encryption schemes (e.g., DES and AES); public key cryptosystems (e.g., RSA and discrete logarithm); and hash functions (e.g., the SHA family). Discusses core information assurance building blocks, such as authentication, digital signatures, key management, and digital certificates. Finally, applies these concepts to important security architectures, including the IP network stack (e.g., IPsec and SSL/TLS), the cellular system, and broadcast media. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.

CY 5130. Computer System Security. 4 Hours.
Offers a practical overview of enterprise computer security, operating systems security, and related topics. Applies concepts such as authentication, access control, integrity, and audit to the modern operating system. Discusses and demonstrates system, process, memory, and file system-level defenses—and the attacks against them. Also discusses topics in data security and virtualization. Uses hands-on labs to reinforce skills and provide practical experience.

CY 5131. Lab for CY 5130. 0 Hours.
Offers small-group laboratory format to cover lab requirements in CY 5130.

CY 5150. Network Security Practices. 4 Hours.
Explores issues involved in the security of computer networks. Topics include firewalls, viruses, virtual private networks, Internet security, and wireless security. Includes case studies and laboratory exercises. Restricted to students in the College of Computer and Information Science or by permission of instructor.

CY 5151. Lab for CY 5150. 0 Hours.
Offers a small-group laboratory format to cover lab requirements for CY 5150.

CY 5200. Security Risk Management and Assessment. 4 Hours.
Creates the opportunity for competency in the development of information security policies and plans including controls for physical, software, and networks. Discusses different malicious attacks, such as viruses and Trojan horses, detection strategies, countermeasures, damage assessment, and control. Covers information system risk analysis and management, audits, and log files. Uses case studies, site visits, and works with commercial products.
CY 5210. Information System Forensics. 4 Hours.
Designed to allow students to explore the techniques used in computer forensic examinations. Examines computer hardware, physical and logical disk structure, and computer forensic techniques. Conducts hands-on experiences on DOS, Windows operating systems, Macintosh, Novell, and Unix/Linux platforms. Builds on basic computer skills and affords hands-on experience with the tools and techniques to investigate, seize, and analyze computer-based evidence using a variety of specialized forensic software in an IBM-PC environment.

CY 5211. Lab for CY 5210. 0 Hours.
Offers a small-group laboratory format to cover lab requirements for CY 5210.

CY 5240. Cyberlaw: Privacy, Ethics, and Digital Rights. 4 Hours.
Describes the legal and ethical issues associated with information security including access, use, and dissemination. Emphasizes legal infrastructure relating to information assurance, such as the Digital Millenium Copyright Act and Telecommunications Decency Act, and emerging technologies for management of digital rights. Examines the role of information security in various domains such as healthcare, scientific research, and personal communications such as email. Examines criminal activities such as computer fraud and abuse, desktop forgery, embezzlement, child pornography, computer trespass, and computer piracy.

CY 5250. Decision Making for Critical Infrastructure. 4 Hours.
Focuses on the art and science of security program management leadership in the context of critical infrastructure protection programs. Includes selected readings, review of decision-making models in crisis, lectures and insights from accomplished leaders in infrastructure protection, and examination of the students’ own unique background and experiences. Trains students on the interaction of vulnerabilities, threats, and countermeasures and how to apply this knowledge to the protection of critical infrastructure using research and analysis of national and global strategies, historical and current legislation, and policies. Also seeks to give students a working knowledge of federal, state, and private-sector critical infrastructure protection resources and programs.

CY 5770. Software Vulnerabilities and Security. 4 Hours.
Seeks to help students to become aware of systems security issues and to gain a basic understanding of security. Presents the principal software and applications used in the Internet, discussing in detail the related vulnerabilities and how they are exploited. Also discusses programming vulnerabilities and how they are exploited. Examines protection and detection techniques. Includes a number of practical lab assignments as well as a discussion of current research in the field.

CY 5976. Directed Study. 1-4 Hours.
Seeks to provide cybersecurity (CY) students with the training experience of working on a specific IA project under the direction of an CY instructor. The instructor provides students with a plan of seminar sessions, including lectures, research, and development of project deliverables and with direction to complete the course. May be repeated without limit.

CY 5978. Independent Study. 2-4 Hours.
Offers independent work under the direction of members of the department on a chosen topic. Course content depends on instructor. May be repeated without limit.

CY 5984. Research. 2-4 Hours.
Offers an opportunity to conduct research under faculty supervision. May be repeated without limit.