Cybersecurity (CY)

Search CY Courses using FocusSearch (http://catalog.northeastern.edu/class-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.

Prerequisite(s): CS 2500 with a minimum grade of D-

CY 2990. Elective. (1-4 Hours)
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

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.

Prerequisite(s): CS 3600 with a minimum grade of D- or CS 3650 with a minimum grade of D-

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.

Attribute(s): NUpath Ethical Reasoning, NUpath Writing Intensive

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.

Prerequisite(s): CS 3600 with a minimum grade of D- or CS 3700 with a minimum grade of D- or CS 4700 with a minimum grade of D- or CS 5700 with a minimum grade of C-

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.

Prerequisite(s): (CS 3000 with a minimum grade of D- ; CS 3800 with a minimum grade of D-) or CS 4800 with a minimum grade of D-
Attribute(s): NUpath Formal/Quant Reasoning

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.

Attribute(s): NUpath Capstone Experience, NUpath Writing Intensive

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.

Attribute(s): NUpath Capstone Experience, NUpath Writing Intensive

CY 4970. Junior/Senior Honors Project 1. (4 Hours)
Focuses on in-depth project in which a student conducts research or produces a product related to the student's major field. Combined with Junior/Senior Project 2 or college-defined equivalent for 8 credit honors in the discipline project.

CY 4971. Junior/Senior Honors Project 2. (4 Hours)
Focuses on second semester of in-depth project in which a student conducts research or produces a product related to the student's major field.

Prerequisite(s): CY 4970 with a minimum grade of D-

CY 5001. Cyberspace Technology and Applications. (4 Hours)
Seeks to provide a systematic understanding of cyberspace technology and applications deployed in the global digital infrastructure. Covers topics in computer networks, server architectures, operating systems, and scripting. All the techniques and tools included in the course are oriented to serve as instruments of security administrators and cybersecurity professionals. Uses practical hands-on labs running on virtual machines and containers hosted in the cloud computing environment to train students. For that reason, a practical overview of virtualization technologies, containerization, and cloud computing models is provided.

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.

Prerequisite(s): CS 2550 with a minimum grade of D- or CY 2550 with a minimum grade of D- or IA 5010 with a minimum grade of C- or CY 5010 with a minimum grade of C- or graduate program admission

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.

Prerequisite(s): CS 2550 with a minimum grade of D- or CY 2550 with a minimum grade of D- or IA 5010 with a minimum grade of C- or CY 5010 with a minimum grade of C- or graduate program admission

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.

Prerequisite(s): CS 2550 with a minimum grade of D- or CY 2550 with a minimum grade of D- or IA 5010 with a minimum grade of C- or CY 5010 with a minimum grade of C- or graduate program admission
Attribute(s): NUpath Ethical Reasoning, NUpath Writing Intensive

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.

CY 6120. Software Security Practices. (4 Hours)
Explores the fundamentals of software security issues from a practical perspective. Takes a deeper dive into the low-level mechanisms used in a variety of most prevalent software security issues and discusses some of the industry best practices needed to address the issues. Offers students an opportunity to learn both an attacker's and defender's perspectives when it comes to software security issue exploitation, detection, and mitigation. Incorporates a number of practical C and assembly coding and lab assignments. Includes an overview of some of the state-of-the-art software security issue exploitation and mitigation techniques used in the field.

Prerequisite(s): CY 5010 with a minimum grade of C-

CY 6121. Lab for CY 6120. (0 Hours)
Offers a small-group laboratory format to cover lab requirements for CY 6120.

CY 6200. Special Topics in IT Security Governance, Risk, and Compliance. (1-4 Hours)
Offers various topics in IT security governance, risk, and compliance. May be repeated for up to 8 total credits.

CY 6240. Special Topics in Privacy Law. (1-4 Hours)
Offers various topics in privacy law. May be repeated for up to 8 total credits.

CY 6720. Machine Learning in Cybersecurity and Privacy. (4 Hours)
Covers a range of theoretical and applied topics related to machine learning uses in security and privacy. Examines vulnerabilities of machine learning and deep learning algorithms and the challenges of securing these systems in real-world applications. Machine learning and AI have enabled a number of critical applications— such as machine translation, speech recognition, and precision medicine—with large positive impact to our daily lives.

CY 6740. Network Security. (4 Hours)
Studies the theory and practice of computer security, focusing on the security aspects of multiuser systems and the Internet. Introduces cryptographic tools, such as encryption, key exchange, hashing, and digital signatures in terms of their applicability to maintaining network security. Discusses security protocols for mobile networks. Topics include firewalls, viruses, Trojan horses, password security, biometrics, VPNs, and Internet protocols such as SSL, IPSec, PGP, SNMP, and others.

CY 6750. Cryptography and Communications Security. (4 Hours)
Studies the design and use of cryptographic systems for communications and other applications such as e-commerce. Discusses the history of cryptographic systems, the mathematical theory behind the design, their vulnerability, and the different cryptanalytic attacks. Topics include stream ciphers including shift register sequences; block ciphers, such as DES and AES; public-key systems including RSA, discrete logarithms; signature schemes; hash functions, such as MD5 and SHA1; and protocol schemes including identification schemes, zero-knowledge proofs, authentication schemes, and secret sharing schemes. Discusses key management problems including Needham-Schroeder protocols and certificates.

Prerequisite(s): CS 5800 with a minimum grade of C- or CS 5800 with a minimum grade of D- or CS 7800 with a minimum grade of C-

CY 6962. Elective. (1-4 Hours)
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

CY 7790. Special Topics in Security and Privacy. (4 Hours)
Offers various topics in security and privacy. May be repeated for up to 8 total credits.

CY 7900. Capstone Project. (4 Hours)
Draws together candidates from diverse backgrounds (technical, legal, and/or law enforcement) in a collaborative activity to address one or more security issues from an integrated perspective. Requires a project proposal, generally industrially oriented, to be submitted and accepted prior to the semester in which the project is to be undertaken.

CY 7962. Elective. (2-4 Hours)
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

CY 7990. Thesis. (2-4 Hours)
Offers selected work with the agreement of a project supervisor. May be repeated without limit.

CY 7995. Project. (1-4 Hours)
Offers students an opportunity to participate in a direct cybersecurity project under the supervision of a faculty member. May be repeated once for a total of 8 credits.

CY 8660. Research Project in National Information 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 technical clients 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. Requires permission of instructor. May be repeated once.

CY 8982. Readings. (1-8 Hours)
Offers selected readings under the supervision of a faculty member. May be repeated without limit.

CY 9000. PhD Candidacy Achieved. (0 Hours)
Indicates successful completion of program requirements for PhD candidacy.

CY 9990. Dissertation Term 1. (0 Hours)
Offers selected work with the agreement of a thesis supervisor.

Prerequisite(s): CY 9000 with a minimum grade of S

CY 9991. Dissertation Term 2. (0 Hours)
Offers dissertation supervision by members of the department.

Prerequisite(s): CY 9990 with a minimum grade of S

CY 9996. Dissertation Continuation. (0 Hours)
Continues work with the agreement of a thesis supervisor.

Prerequisite(s): CY 9991 with a minimum grade of S or Dissertation Check with a score of REQ