Bellevue University Cybersecurity Programs & Courses

Undergraduate
Course List

Core Courses:
- CYBR 250 Introduction to Cyber Threats, Technologies and Security
- CIS 311 Network Security
- CIS 312 Securing Access Control
- CIS 411 Assessments and Audits
- CYBR 320 Operational Security
- CYBR 340 Operating Systems and Mobile Device Security
- CYBR 350 Web, Commerce and Application Security
- CYBR 410 Data/Database Security
- CYBR 420 Cyber Investigations and Forensics
- CYBR 450 Advanced Cybersecurity Concepts

Plus, choose two courses (6 credit hours) from the following:
- CIS 242 Introduction to Programming using Java
  OR
- CIS 243 Introduction to Programming Using C#
- CIS 313 Cryptography
- CIS 321 Structured System Analysis and Design
- CIS 351 Networking Structures and Desktop Operating Systems
- CIS 357 Operating System Administration
- CIS 433 Information Technology Project Management
- CIS 436 Ethics for IT Professionals
  OR
- CIS 468 Accounting for IT Professionals
- AC 341 Accounting Information Systems
- PS 208 Introduction to National Security
- PS 209 Foundations in Intelligence and Counterintelligence
- PS 210 Ethical Controversies in Security and Intelligence
- CYBR 433 Security for Business, Finance, and Accounting
- CYBR 436 Security for Healthcare
Bellevue University Cybersecurity Programs & Courses

This course introduces information technologies and examines methods for protecting them against persistent and constantly evolving threats. Existing and emerging information technologies are discussed including operating environments, computer networking, and data management. Basic methods for managing information systems and technologies are presented from a standpoint of providing sufficient security protections.

CIS 311 Network Security

This course provides an introduction to the goals, functional processes, tools, and techniques associated with network security. Discussion includes devices such as firewalls, intrusion detection mechanisms, and Virtual Private Networks (VPNs). Telecommunications and network security protocols used to prevent, detect, and correct potential vulnerabilities associated with both the outsider and insider threat are also explored.

CIS 312 Securing Access Control

This course provides an introduction to the concepts associated with configuring identification and authentication. Discussion includes comparison of various access models, and how passwords, smart cards and biometric devices can assist in securing system access and ensure confidentiality, integrity, and availability of data. Other technologies such as remote authentication and Public Key Infrastructure (PKI) are also explored.

CIS 313 Cryptography

This course provides an introduction to the fundamental components of encryption. Topics include the history of cryptography, public key and private key systems, hashing, and digital signatures. Topics also include the development of the Advanced Encryption Standard, the use and functionality of Pretty Good Privacy, and the Secure Socket Layer.

CIS 411 Assessments and Audits

This course explores the principles of risk assessment, vulnerability analysis, and auditing. Discussion includes the use of these principles to evaluate the effectiveness of information security controls. Topics include threat and asset identification, countermeasures and safeguards, acceptable risks, and vulnerabilities. The auditing concepts of technical, physical, and administrative controls are also introduced along with how these controls are measured for effectiveness.

CYBR 320 Operational Security

This course focuses on the skills required to operate a security program within an organization. Coverage includes the practical application of security practices in an operational environment. Topics include security structure, leading security projects, policy management, human factors of security, and physical security methods.

CYBR 340 Operating Systems and Mobile Device Security

This course focuses on the skills required to secure base operating systems on server, desktop, virtual, and mobile platforms. Coverage includes the practical application of security tools, utilities, and
configurations for protecting computer operating systems at both the user and corporate level. Discussion also includes protecting stand-alone and virtualized servers, cloud computing security, and the protection of mobile platforms such as smart phones, tablets and handheld computers.

CYBR 350 Web, Commerce and Application Security

This course explores securing core technologies that support Internet applications and commerce. Processes for creating and administering Internet web sites to ensure proper protections are introduced. The course also addresses securing applications on Internet websites and mobile platforms, and introduces basic methods for secure development.

CYBR 410 Data/Database Security

This course focuses on the protection of data at rest. Coverage includes the identification, ownership, and protection of data – whether residing in files, folders, or databases. This course also introduces the concept of database security to include: Architecture, Password Policies, Auditing, Privileges, and Roles Administration. Emphasis is placed on areas unique to data and database security.

CYBR 420 Cyber Investigations and Forensics

This course examines basic methods of investigation, information acquisition, and management of Internet and computer forensic cases. Topics include record-searching, note taking and report writing, and using scientific methodology in Cyber investigations. Coverage also includes basic tools and techniques for forensic analysis of computers, networks systems, and mobile devices.

CYBR 450 Advanced Cybersecurity Concepts

This course provides a monitored structure for application of the skills and knowledge acquired throughout the Cybersecurity program. Emphasis is placed on the use of real-world security problems, issues, and situations. Course assignments will require the use of protection, detection, deterrence, and response techniques in addressing threats, vulnerabilities, and risks found in businesses today.
Bellevue University Cybersecurity Programs & Courses

Graduate
Course List

Core Courses:
- CIS 607 Computer Forensics
- CIS 608 Information Security Management
- CYBR 510 Physical, Operations, and Personal Security
- CYBR 515 Security Architecture and Design
- CYBR 520 Human Aspects of Cybersecurity
- CYBR 525 Ethical Hacking and Response
- CYBR 610 Risk Management Studies
- CYBR 615 Cybersecurity Governance and Compliance
- CYBR 650 Current Trends in Cybersecurity

Plus, choose three courses (9 credit hours) from the following:
- CIS 519 IT Strategy and Policy
- CIS 520 Survey of System Development
- CIS 537 Introduction to Cyber Ethics
- CIS 605 Advanced Database Management
- PS 639 Cyberwar or Cyberdeterrence
  OR
- CIS 610 Information Warfare
- CIS 611 Cloud computing
- CIS 629 Managing Emerging Technologies
- CIS 633 Information Security Technology Project Management
- CYBR 545 White collar Crime
- CYBR 613 Control System Security
- CYBR 625 Business Continuity Planning and Recovery
- CIS 644 Managing Project Risks
- MHA 602 Health Information Technologies and Administration

CIS 607 Computer Forensics

This course is designed as an overview of the investigative methods and tools associated with computer forensics. Topics include: processing crime and incident scenes, digital evidence controls, recovery of information, network forensics, data acquisition, and legal and ethical issues associated with investigations.
Bellevue University Cybersecurity Programs & Courses

CIS 608 Information Security Management

This course addresses the issues relating to successful information security management. Topics include access control systems, network and software security, management practices, risk management, protection mechanisms, business continuity planning, and legal and ethical issues. The course allows for analysis of current security management models.

CYBR 510 Physical, Operations, and Personnel Security

This course presents an examination of effective security methodologies based on comprehensive assessment of threats and implementation of a layered system of physical and electronic protection. Threat identification, countermeasures, and prevention are explored.

CYBR 515 Security Architecture and Design

This course provides an introduction to the fundamental components of security architecture. Topics include computer organization; hardware, software and firmware components; open and distributed systems; and protection mechanisms. Discussion also includes certification and accreditation; formal security models; and evaluation criteria. Assigned projects include designing a model secure system.

CYBR 520 Human Aspects of Cybersecurity

This course provides an exploration of the human aspects of Cybersecurity. Topics include human behavior and interaction; motivation and influence; and social engineering. Emphasis is on the human element of cyber incidents in relation to protecting information and technology assets.

CYBR 525 Ethical Hacking and Response

This course provides a technical study of offensive and defensive techniques for protecting cyber assets. Topics include security testing, risk mitigation techniques, and threat response. Discussion also includes penetration testing theory, techniques, and tools; network, systems, and application vulnerability scanning; risk analysis and response; and intrusion detection and response. Emphasis is placed on identification of system vulnerabilities and threats and techniques for preventing attacks.

CYBR 610 Risk Management Studies

This course provides a technical study of offensive and defensive techniques for protecting cyber assets. Topics include security testing, risk mitigation techniques, and threat response. Discussion also includes penetration testing theory, techniques, and tools; network, systems, and application vulnerability scanning; risk analysis and response; and intrusion detection and response. Emphasis is placed on identification of system vulnerabilities and threats and techniques for preventing attacks.

CYBR 615 Cybersecurity Governance and Compliance

This course provides an exploration of the governance of information systems. Discussion includes the importance of compliance with laws, regulations, policies, and procedures as a means of minimizing risk through mandated security and control measures.
Bellevue University Cybersecurity Programs & Courses

CYBR 650 Current Trends in Cybersecurity

This course presents an in-depth study of current trends in Cybersecurity threats. Discussion includes the identification and management of threats and vulnerabilities within an effective enterprise security program. Prior Cybersecurity education is synthesized through projects and assignments.

CYBR 625 Business Continuity Planning and Recovery

This course provides an introduction to the processes associated with business continuity planning and disaster recovery. Topics include project scope and planning, assessing risk, developing policy and procedures, and conducting a business impact analysis. Discussion also includes disaster recovery plan development and implementation, and restoration.