Graduate Certificate in Cybersecurity Management

Securing an organization's data requires a combination of technical skills, innovative concepts and managerial acumen. The Graduate Certificate in Cybersecurity Management at Washington University is a 15-unit part-time program designed for working professionals. This program was developed with one critical goal: to educate professionals about how to manage the people and resources required to perform these tasks and to lead the cybersecurity functions of various organizations.

The curriculum provides students with the knowledge needed to protect from, defend against, respond to and recover after cyber threats. Graduates of this certificate program will be equipped to design, engineer and assess global cybersecurity problems while maintaining the vision and strategy of the enterprise.

Graduate Certificate: 15 units, 10-15 months to complete

Email:	sever@wustl.edu
Website:	https://sever.wustl.edu/degree-programs/cybersecurity/index.html

Faculty

Program Director

Joe Scherrer (https://sever.wustl.edu/faculty/Pages/Joe-Scherrer.aspx)
Executive Director, Professional Education
Director, Cybersecurity Strategic Initiative
Program Director, Graduate Studies in Cybersecurity Management
Doctor of Liberal Arts, Washington University in St. Louis, 2023 (projected)
MS, Business Administration, Boston University
MS, Information Systems Management, Air Force Institute of Technology
MS, National Security Studies, Naval War College
MS, Strategic Studies, Air War College
BS, Electrical Engineering, Washington University in St. Louis

For a list of our program faculty (https://sever.wustl.edu/faculty/#cybersecurity_management), please visit our website.

Requirements

Graduate Certificate in Cybersecurity Management

Total units required: 15

In order to earn the certificate, all courses must be passed with a C- or higher. In addition, a student must have a cumulative grade-point average of at least 2.70 over all courses applied toward the certificate.

Code	Title	Units
Required: 15 units		
CYBER 560	Cybersecurity Technical Fundamentals	3
CYBER 561	Oversight for Excellence: Cybersecurity Management and Governance	3
CYBER 562	Efficient and Effective Cybersecurity Operations	3
CYBER 566	Cybersecurity Risk Management	3
CYBER 567	The Hacker Mindset: Cyber Attack Fundamentals	3

Courses

Visit online course listings to view semester offerings for T83 CYBER (https://courses.wustl.edu/CourseInfo.aspx?sch=T&dept=T83&crslvl=5:8).

T83 CYBER 560 Cybersecurity Technical Fundamentals
This course presents a comprehensive survey of cybersecurity technology, including basic theory and concepts. Students will gain hands-on familiarity with cybersecurity technology through lab exercises, in-class studios, and scenarios. Topics covered include security considerations surrounding operating systems, the web, email, databases, wireless technology, the cloud, and the Internet of Things. Also addressed are cryptography, secure software design, physical security, and human factors in cybersecurity.
Credit 3 units.

T83 CYBER 561 Oversight for Excellence: Cybersecurity Management and Governance
This course takes a comprehensive approach to the management of the organizational cybersecurity function. It also explores the principles of information technology governance. Course work provides a deeper understanding of best practices for managing cybersecurity processes and meeting multiple needs of enterprise management by balancing business risks and operational and technical imperatives. Toward this end, the course addresses a range of topics necessary for success, including the elements of and how to establish a governance program, cybersecurity management frameworks, developing and implementing a cybersecurity strategy, deploying cybersecurity policy and controls, ensuring standards and regulatory compliance, functional and budgetary advocacy, interfacing with the C-suite and board, and talent acquisition and development.
Credit 3 units.

T83 CYBER 562 Efficient and Effective Cybersecurity Operations
In this course, students will gain understanding of what it takes to manage the people, process, and technology for effective and efficient day-to-day cybersecurity operations. Using the Cybersecurity Operations Center (CSOC) as the fundamental exemplar, students will learn the functions and processes that comprise a typical CSOC with an underlying focus on continually optimizing operations and processes to ensure agility and performance. Students will examine options for structuring the CSOC and core CSOC functions and processes such as threat intelligence; monitoring, detection, and threat

assessment; vulnerability management; incident response; prevention, including awareness training; partner and third-party coordination; analytics, metrics, and reporting; training; and CSOC technologies and instrumentation.
Credit 3 units.

T83 CYBER 566 Cybersecurity Risk Management
In this course, students will gain deeper appreciation of the challenges faced by enterprises when addressing cybersecurity risks. The course will cover the evolution of cyber threats, including attacker methods and their targets across different industries. Students will be able to understand the differences between enterprise, operational and cybersecurity risk management and the role that each play (or should play) in managing risks to an organization. Students will gain technical understanding of industry-leading frameworks (COSO, ISO, NIST, FAIR) and become conversant with their strengths and weaknesses as well as the applicability and practicality of their implementation.
Credit 3 units.

T83 CYBER 567 The Hacker Mindset: Cyber Attack Fundamentals
This course is designed to provide an introductory understanding of how offensive security techniques practically operate. During this course, students will use hacking techniques to compromise systems, collect data, and perform other tasks that fall under the generally understood use of the term "hacker." These techniques will be related to risk-based defensive security practices, with a view toward enhancing the student's understanding of what it takes to be a successful "defender." By the conclusion of the course, students will have a baseline technical understanding of hacking techniques; they will have executed offensive security operations and increased their technical understanding of what it takes to deal with cyber threats.
Credit 3 units.