Washington University in St. Louis

Master of Cybersecurity Management

Securing an organization's data requires a combination of technical skills, innovative concepts and managerial acumen. The Master of Cybersecurity Management at Washington University is a 30-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 program will be equipped to design, engineer and assess global cybersecurity problems while maintaining the vision and strategy of the enterprise.

Part-time Master's Degree: 30 units, 2.5 years+ 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

Master of Cybersecurity Management

Total units required: 30

In order to earn the degree/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 degree/certificate.

Code	Title	Units
Required: 21 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
CYBER 587	Cloud Security	3
INFO 570	Leadership Seminar for Technology Professionals	3
Electives: Choose 9 units		
Cybersecurity Management Emphasis		
CYBER 563	Enterprise Network Security	3
CYBER 564	Access Control and Identity Management	3
CYBER 565	Cybersecurity Analytics	3
CYBER 568	Emerging Issues and Technology in Cybersecurity	3
CYBER 569	Incident Response and Business Continuity	3
CYBER 570	Managerial and Technical Approaches to Cybersecurity Assurance	3
Cybersecurity Design & Engineering Emphasis		
Offered through the Computer Science & Engineering department for those with the appropriate STEM background		
CSE 433S	Introduction to Computer Security	3
CSE 523S	Systems Security	3
CSE 569S	Recent Advances in Computer Security and Privacy	3
CSE 571S	Network Security	3
CSE 637S	Software Security	3
Bridge Course*		
CYBER 559	Introduction to Cybersecurity	3

* The bridge course is offered for students with limited to no cybersecurity background. The successfully completed course will count toward the 9 required elective units.

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 559 Introduction to Cybersecurity
This course is intended as a comprehensive introduction to the cybersecurity field. It covers a broad range of cybersecurity terms, definitions, historical perspectives, concepts, processes, technologies, and trends, with a focus on managing risk and the employment of cybersecurity as an organizational enabler.
Credit 3 units.

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 563 Enterprise Network Security
This course presents a detailed and comprehensive study of the architecture and defensive approaches to protect enterprise network environments against cyber threats. Students will gain practical experience in secure network architectures and design approaches. Using a building-block approach along with case studies and design exercises, the course will establish the value of applied foundational security frameworks and system models. Specific topics include defensive network design, advanced treatment of appropriate security implementation tools and techniques, boundary defense, secure wireless and mobility solutions, remote and business partner access, and third-party and vendor interactions to ensure appropriate enterprise network solutions are implemented.
Credit 3 units.

T83 CYBER 564 Access Control and Identity Management
Business advancements due to technologies such as cloud, mobility, and the need to access information from anywhere using any device have made identity management and access control a critical component of cybersecurity. In this course, students will gain understanding of organizational and technical identity management and access control frameworks. They will also learn central concepts such as least privileged access, authentication, and authorization, which protect applications and systems from unapproved access. Topics covered include single sign-on, privileged account management, provisioning, role management, and directory services. Students will complete a "real-world" identity management and access control business case to identify risks and controls, and they will also create a strategy and roadmap to address challenges and propose solutions.
Credit 3 units.

T83 CYBER 565 Cybersecurity Analytics
This course provides an introduction to use of data analytics in support of an organization's cybersecurity function. The course is designed to increase student understanding of how data analytics can be used to manage security and how data analytics can be deployed in support of risk-based assessment and decision making. Students who complete this course successfully will be able to apply data analytics techniques and tools to help organizations discover anomalies pertaining to cyber threats; to implement, assess and monitor basic security functions; to respond to emerging threats or prioritized requests as defined by organizational stakeholders; to depict cybersecurity risk posture within the context of compliance and regulatory requirements; and to construct a comprehensive cybersecurity analytics framework.
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.

T83 CYBER 568 Emerging Issues and Technology in Cybersecurity
Each new technology advancement brings with it promises and challenges. Will it be used for good or lead to disaster? This course examines contemporary and near-future cybersecurity threats and the potential security impact of new technologies. Topics include new

forms of computing and communications and their implications for cybersecurity practitioners as well as incipient threat vectors. Historical security incidents will also be used to provide context and insight into the relationship of technology and security. Throughout the course, students will be challenged to develop strategies and responses to deal with emerging technologies and threats in the ever-evolving cybersecurity domain.
Credit 3 units.

T83 CYBER 569 Incident Response and Business Continuity
This course focuses on the end-to-end process and methods to deal with cybersecurity incidents. Using recent examples of cyber breaches and incidents, students explore how CISOs react and respond to these incidents and learn best practices for doing so. Topics include developing an incident response plan, organizing an incident response team, leveraging cyber intelligence and external partners to aid in response, handling public and private communications about the incident, and post-breach restoration. Particular attention will be paid to establishing a strong understanding of cybersecurity indicators and motives for espionage activities from both an external and rogue insider's perspective. Students will learn about host-based and network incident response tools and digital forensic tools, including techniques and tactics for their effective use. This section of the course includes key "hands-on" activities that are typically used in post-breach analysis and investigations, such as the forensic analysis of network storage, hard drives, and memory. Students will also become familiar with post-breach report construction and examine the proper drafting and use of such reports for submission to legal counsel, the courts, and organizational leaders.
Credit 3 units.

T83 CYBER 570 Managerial and Technical Approaches to Cybersecurity Assurance
How do you know if your organization is secure? How do you communicate your security posture to those who don't have expertise in cybersecurity? Many organizations fall woefully short in answering these questions. Too often gut feel takes the place of data-driven evidence of security. As a cybersecurity professional you are responsible to ensure your organization is secure and that you communicate your security posture with confidence to non-practitioners, especially your senior leadership and the board. This course provides you the concepts, methods, tools, and intellectual framework to achieve cybersecurity assurance and how you as cybersecurity leaders communicate that assurance to the C-suite and the board. Topics covered include adopting a cybersecurity maturity model, metrics selection and development, the critical role of internal and external security assessments and compliance audits, vulnerability management as a foundation of cybersecurity assurance, and how to effectively employ red/blue team activities.
Credit 3 units.

T83 CYBER 587 Cloud Security
TToday's organizations are more and more focused on delivering faster results and better products and services and doing this securely in an ever-evolving technological landscape. Cloud-based technologies have enabled the critical capabilities, functionality and innovations necessary to transform the way organizations survive and thrive in this competitive environment. As such, "the cloud" requires cybersecurity practitioners to think differently about managing risk, producing resilient solutions, and dealing with third-party providers. In this course, students will learn best practices for cloud security to include methods for architecting and applying security-related features in a cloud platform. Through case studies, standards, best practices, and studio exercises, students will develop the necessary skills to identify the security challenges of a cloud environment in support of the ongoing operations of the enterprise.
Credit 3 units.

T81 INFO 570 Leadership Seminar for Technology Professionals
This seminar is designed to develop the leadership capacity of professionals working in the information technology (IT) and cybersecurity fields. Although domain expertise plays an important role in the success of a technology professional, it is when this expertise is integrated with the ability to lead people that transforms the merely competent into multidimensional force multipliers for the organization. In this course, students will participate in an immersive seminar-based learning experience targeted toward professional and personal development on a range of essential leadership skills. Students will benefit from interaction with industry experts in the IT and cybersecurity fields and receive coaching support to achieve professional and personal goals. Each student will complete a series of self-assessments and multi-rater assessments as well as a personal leadership development plan to gain insight and build competencies critical to effective leadership. Topics include creating a shared vision, strategy development, building and sustaining a healthy culture, essentials of finance and budgeting, driving results, energizing people for performance, innovation, emotional intelligence, navigating organizational politics, managing up, negotiations, stress resilience, talent coaching and development, effective communication, and time management.
Credit 3 units.