The Executive Master in Cybersecurity

Strategy is the Best Security

The Brown University Executive Master in Cybersecurity (EMCS) is an 18-month master's degree for professionals designed to cultivate high-demand, industry executives with the unique and critical ability to devise and execute integrated, comprehensive cybersecurity strategies for nations and industries across the globe.

Leveraging Brown's culture of interdisciplinary study and cybersecurity excellence, the program fosters industry leaders prepared to address cybersecurity's global, technical, human, and policy challenges. The program convenes world-class thought leaders from Brown's top-ranked Department of Computer Science and Watson Institute for International and Public Affairs.

The program features hands-on assessments of cyber vulnerabilities, attacks, and defenses. Students devise actionable plans to address real-time cybersecurity challenges in their own organizations.

Students graduate armed with a powerful professional network and cross-industry expertise to meet the global demand for cybersecurity leadership.

Participant Profile

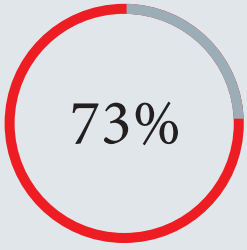
EMCS is an intensive masters program for mid-career cybersecurity professionals who seek a broader perspective to help position their organizations for optimal security.

Participants demonstrate a strong track record of achievement, have diverse backgrounds, and come from various cybersecurity related sectors.

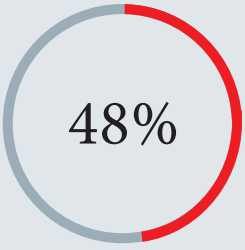
This 18-month program is delivered in a blended format, combining online learning with five face-to-face residential sessions.

Brown Executive Programs deliver real outcomes.

ALUMNI WHO GRADUATED READY TO LEAD



ALUMNI PROMOTED TO ADVANCED LEADERSHIP OR C-SUITE ROLES



STUDENTS PROMOTED WHILE STILL IN THE PROGRAM

GAIN THE NETWORK AND KNOWLEDGE TO DRIVE FORWARD CHANGE IN YOUR CAREER AND ORGANIZATION

brown.edu/cybersecurity



Designed to deliver a transformational experience with courses in:

Introduction to Computer Security
Engage with an array of privacy and security issues for computers, mobile devices, and networks. The course covers principles and skills useful for making informed security decisions and for understanding how security interacts with the world around us.

Global Cyber Challenges: Law, Policy, and Governance
Examine a variety of cybersecurity law and policy issues which range from private sector information sharing and critical infrastructure protection to cyber crime, internet governance, and international law as it might apply in a cyber conflict

Privacy and Personal Data Protection
Gain practical experience with the development of modern privacy law around the world, and the current US legal and regulatory framework— including protection of personal health, financial, educational, workplace, and other personal data.

Human Factors: People and Software
Discover a richer understanding of the strengths and weaknesses of human agents and their interaction with software systems, and thus how they are central to cybersecurity problems. Projects include case studies on security as it relates to: business workflows, trade-offs with usability, system configuration, and the detection of insider threats.

Applied Cryptography and Data Privacy
Explore the concepts of provable security and study basic cryptographic topics such as encryption, digital signature schemes, zero-knowledge proofs and differential privacy.

Effective Leadership
Students will prepare to assume greater leadership roles in their organizations by developing and reinforcing critical skills such as persuasive communication, management of change, negotiation, conflict resolution, and ethics.

Management of IT Systems and Cybersecurity Risks
Analyze the practical challenges facing executives of business organizations in managing information technology systems and cyber risks. This course focuses on the costs and tradeoffs that are involved in all security and privacy decisions.

Advanced Topics in Computer Security
Advanced security topics are introduced through real-life examples that are relevant to today's organizations, from small business to global enterprises. Course topics include multifactor authentication frameworks and systems; mobile operating systems and application security; malware detection and intrusion detection; security and privacy in cloud computing and storage; security, privacy, and fairness in machine learning.

The Future of Cybersecurity: Technology and Policy
Explore operational security, product development and acquisition, securing enterprise computing, and human factors. Students will also examine corporate issues that are likely to arise at the national and international levels.

The Critical Challenge: Capstone Project
The Critical Challenge Project (CCP) is central to the Executive Master in Cybersecurity. Under the direction of a faculty member, the student identifies and analyzes a critical challenge respective to their organization from multiple perspectives and develops a comprehensive plan for addressing it.

BROWN

EXECUTIVE MASTER IN
CYBERSECURITY

Contact us:
Execmasters@brown.edu
401-863-2700

brown.edu/cybersecurity