MIT MANAGEMENT
EXECUTIVE EDUCATION

CYBERSECURITY FOR MANAGERS: A PLAYBOOK

BUILD YOUR ACTION PLAN FOR
A MORE CYBER RESILIENT ORGANIZATION.

Delivered in collaboration with EMERITUS

OVERVIEW

When a security breach happens, the disruption and damage can vary widely. But one thing is for certain: the effects ripple through the entire organization, often having significant operational and financial implications.

Creating a cybersecure organization is a necessary goal today. Decisions about cybersecurity have implications throughout your organization—not only for technology-focused teams, but for every team. Sophisticated phishing schemes, ransomware, and data breaches are on the rise, and their level of complexity is increasing. Therefore, all of us have a role to play in keeping our organization secure.

In this program, you will learn:

- How to select and use the right frameworks to enhance cybersecurity decision-making in your organization
- How to assess risk, improve defenses, and reduce vulnerabilities in your organization
- How to speak the language of cybersecurity to enable informed conversations with your technology teams and colleagues, and ensure your organization is as cybersecure as possible

START DATE

December 19, 2019

PRICE

$2,800*

DURATION

6 week, excluding orientation
5-6 hours/week

*GST applicable to Singapore residents.

IMPACT

Upon completion of the program, participants will be equipped with:

- A framework that provides a strategic view of an organization's cybersecurity risk management, including management mechanisms you can put in place immediately
- A playbook with actionable next steps for improving a culture of cyber awareness within your organization
- The language and vocabulary to support informed conversation with your CISO, CTO, and other technology leaders
- An appreciation of how decisions made by technologists may affect the business landscape within your organization
- An awareness of the leading approaches to managing cybersecurity, including 'defense in depth' and the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- A practical interpretation of the tradeoffs between security and privacy, and a method for understanding your organization's priorities

WHO SHOULD ATTEND

This online program is for business leaders, general managers, and executives looking to build an action plan for a more cyber resilient organization. Technology and business consultants and others acting as liaisons between technology and business units will also benefit.

Industry examples cited in the program include:

- Technology
- Financial services
- Insurance industry
- Manufacturing
- Retail
- Telecommunications
- Government organizations

PAUL MCDONAGH-SMITH

Digital Capability Leader at MIT Sloan

"In MIT Sloan online programs, we aim to build both capability and confidence. Insights are supported by real-world examples and opportunities to apply what you are learning."

PROGRAM HIGHLIGHTS

Cybersecurity for Managers: A Playbook is an engaging, interactive, and personalized learning experience, built upon learning tools which include:

A Personalized Cybersecurity Playbook:

- Bring together key concepts and insights from the program modules to build an action plan—a playbook—of what you will do next

Case Studies and Examples:

- Insurance case study on creating a culture of prevention and awareness
- Manufacturing case study featuring the NIST Cybersecurity framework
- Ethics considerations in cybersecurity explored through a case study involving Apple Inc.

Interactive Cybersecurity Simulation:

- Test out different budget scenarios for prevention, detection, and response – and learn how each affects profitability

Industry Perspectives:

- In depth interview with a cloud cybersecurity industry expert

PROGRAM MODULES

This program integrates rich, interactive media including videos and a simulation, as well as traditional components such as individual assignments. The program design facilitates collaborative learning through discussion forums and live office hours. This results in an enhanced peer network that delivers value long after the program ends.

ORIENTATION MODULE

Welcome to Your Online Campus

Receive an overview of the learning platform, including how to access videos, engage in discussion groups, submit application exercises, and contact your delivery support team.

MODULE 1

Understanding the Threat Landscape

Gain an overview of the key concepts and practices in cybersecurity.

- Dispel common myths such as 'cybersecurity is just an IT problem'
- Cyber safety: applying accident research to prevent cyber incidents
- IoT: how expanding connectedness opens the door to cyber threats

MODULE 2

Organizing Cyber Management Priorities: The NIST framework

Use the High-Tek Sensors case to learn about the NIST Cybersecurity Framework and apply key concepts to individual organizations.

- Interactive case study: High-Tek Sensors (manufacturing)
- NIST Cybersecurity Framework
- Applying NIST to your organization

MODULE 3

Measuring Risk Exposure

Identify risk and use frameworks for measuring risk.

- Overview of risk management practices
- Qualitative and quantitative frameworks for measuring risk
- Cyber insurance: risk transfer

MODULE 4

Improving Defenses with Systems and Technology

Learn the basics of cybersecurity resource allocation and the concept of ‘defense in depth’.

- Vulnerabilities and security
- Simulation of cybersecurity funds budgeting
- Interview with a cloud cybersecurity expert on ‘defense in depth’

MODULE 5

Building a Culture of Cybersecurity

Learn about management mechanisms for influencing cybersecurity culture within organizations.

- The Cybersecurity Culture Model
- Interactive case study: insurance company
- Practical steps for achieving organizational security

MODULE 6

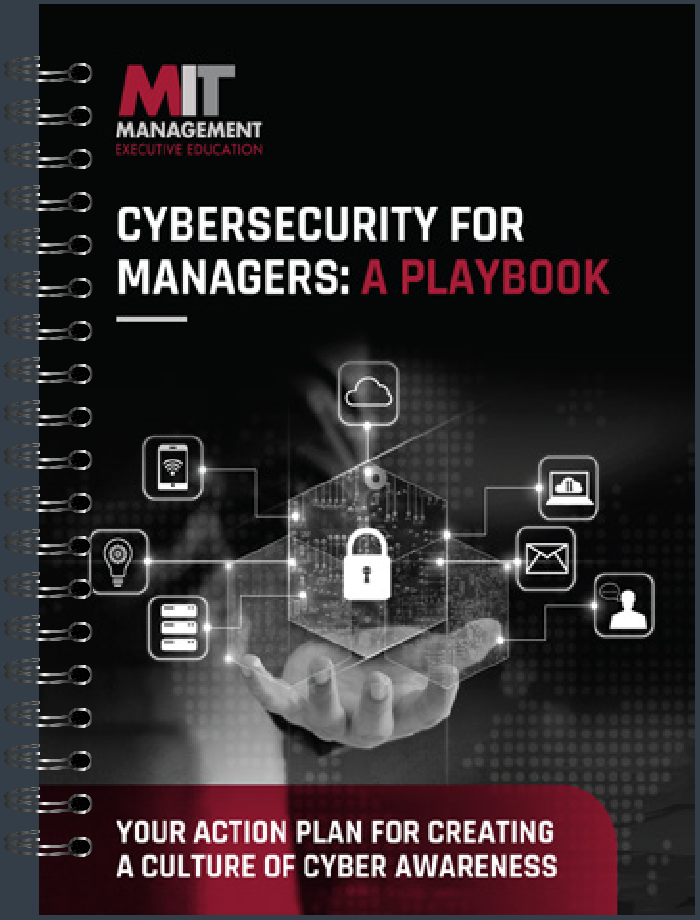
Exploring Ethics in Cybersecurity

Understand important tradeoffs between security and privacy.

- Considerations of ethics in cybersecurity using the Apple-FBI controversy as an example
- Faculty roundtable discussion

YOUR PLAYBOOK

Developing an Action Plan for Your Organization



MIT MANAGEMENT EXECUTIVE EDUCATION

CYBERSECURITY FOR MANAGERS: A PLAYBOOK

YOUR ACTION PLAN FOR CREATING A CULTURE OF CYBER AWARENESS

Note: Participants can print their playbook at the end of the program to have a takeaway resource.

In this program, we will cover a number of items to assist in the management and leadership of cybersecurity in organizations. We bring together key concepts from the learning modules to create an action plan—a playbook—of what you will do next. This will enable you to have more informed conversations with your CISO or other technology leaders.

Each module includes an exercise designed to allow you to apply key concepts and insights to your own situation.

By using the playbook, you will be able to:

- Apply concepts from the program to your organization.
- Create a list of actionable activities to implement in your work, teams, and organization from this point forward.

PROGRAM FACULTY

Stuart Madnick

John Norris Maguire (1960) Professor of Information Technology; Professor, Information Technology and Engineering Systems; Co-Director, PROFIT Program

Stuart Madnick is the John Norris Maguire Professor of Information Technologies at the MIT Sloan School of Management, a Professor of Engineering Systems at the MIT School of Engineering, and the Founding Director of Cybersecurity at MIT Sloan: the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Madnick's involvement in cybersecurity research goes back to 1979, when he coauthored the book Computer Security. Currently he heads the Cybersecurity at MIT Sloan initiative, formerly called the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, aka (IC)3.

Keri Pearlson

Executive Director, Cybersecurity at MIT Sloan

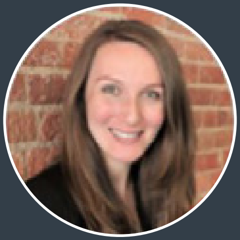
Keri Pearlson is the Executive Director of Cybersecurity at MIT Sloan and has held positions in academia and industry including Babson College, The University of Texas at Austin, Gartner's Research Board, CSC, and AT&T. She founded KP Partners, a CIO advisory services firm and the IT Leaders' Forum, a community of next generation IT executives. She is the founding director of the Analytics Leadership Consortium at the International Institute of Analytics. Pearlson began her career at Hughes Aircraft Company as a systems analyst.

Dr. Michael Siegel

Director of Cybersecurity at MIT Sloan (CAMS) and Principal Research Scientist

Dr. Michael Siegel is a Principal Research Scientist at the Sloan School of Management, Massachusetts Institute of Technology. He is also the Director of Cybersecurity at MIT Sloan (CAMS). Dr. Siegel's research focuses on the management, strategy, technology, and organizational issues related to cybersecurity with specific interest in vulnerability markets, cyber risk metrics, dark web business models, IoT endpoint security, cybersecurity workforce development, and educating management in cybersecurity. He also has done research in the intelligent integration of information systems, risk management, insurgency and state stability, data analytics, healthcare systems, and systems modeling. Dr. Siegel has published articles on such topics as simulation modeling for cyber resilience, cyber vulnerability markets, data management strategy, architecture for practical metadata integration, heterogeneous database systems, and managing and valuing a corporate IT portfolio using dynamic modeling of software development and maintenance processes. His research at MIT has continued for over 30 years and includes a wide range of publications, patents and teaching accomplishments.

WHAT PARTICIPANTS SAY

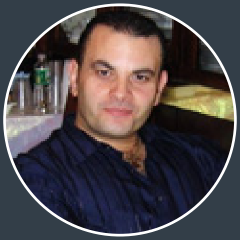


“I have a much better understanding of the types of threats I need to consider for my company, including some jargon I didn't previously understand. I loved the sections on building a culture of security and I am actively implementing some of those ideas.”

- Sarah Taylor, General Manager at Research Square
USA

“I really liked the simulation of applying costs for cybersecurity, and the discussion about the Apple case. It makes one realize the number of layers affected when such incidents happen.”

- Bruno Schmid, Senior Security Engineer at Avectris
SWITZERLAND



“The best part is the videos and especially discussions. Applying what you have learned at the same time as learning from other students' points of view.”

- Simon Mzaouakk, VP- Technology Officer at Watertown Savings Bank
USA

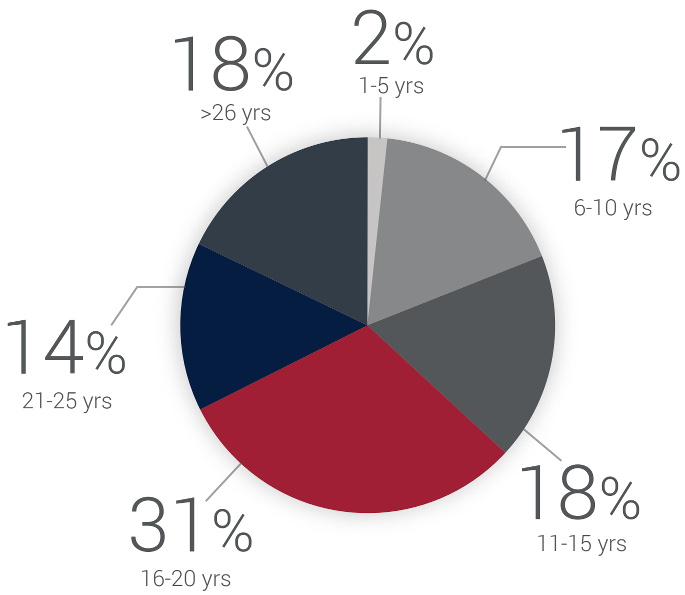
“Interactions with the class participants and simulations helped me understand what like-minded professionals face in their cybersecurity related challenges.”

- Heng Chye Carter Tan, Enterprise Solutions Architect at
Keppel Enterprise Services
Singapore

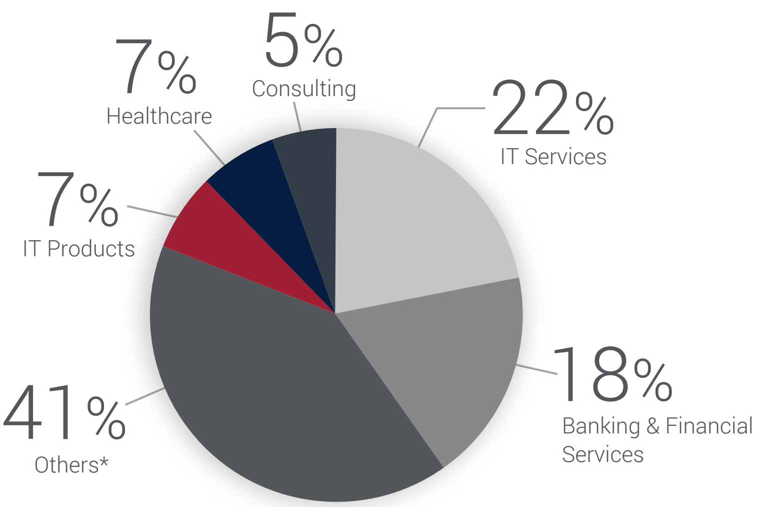
PARTICIPANT PROFILE

Past participants come from a wide range of industries, job functions, and management levels—from more than 33 countries around the world.

Participants by Years of Experience



Participants by Industry



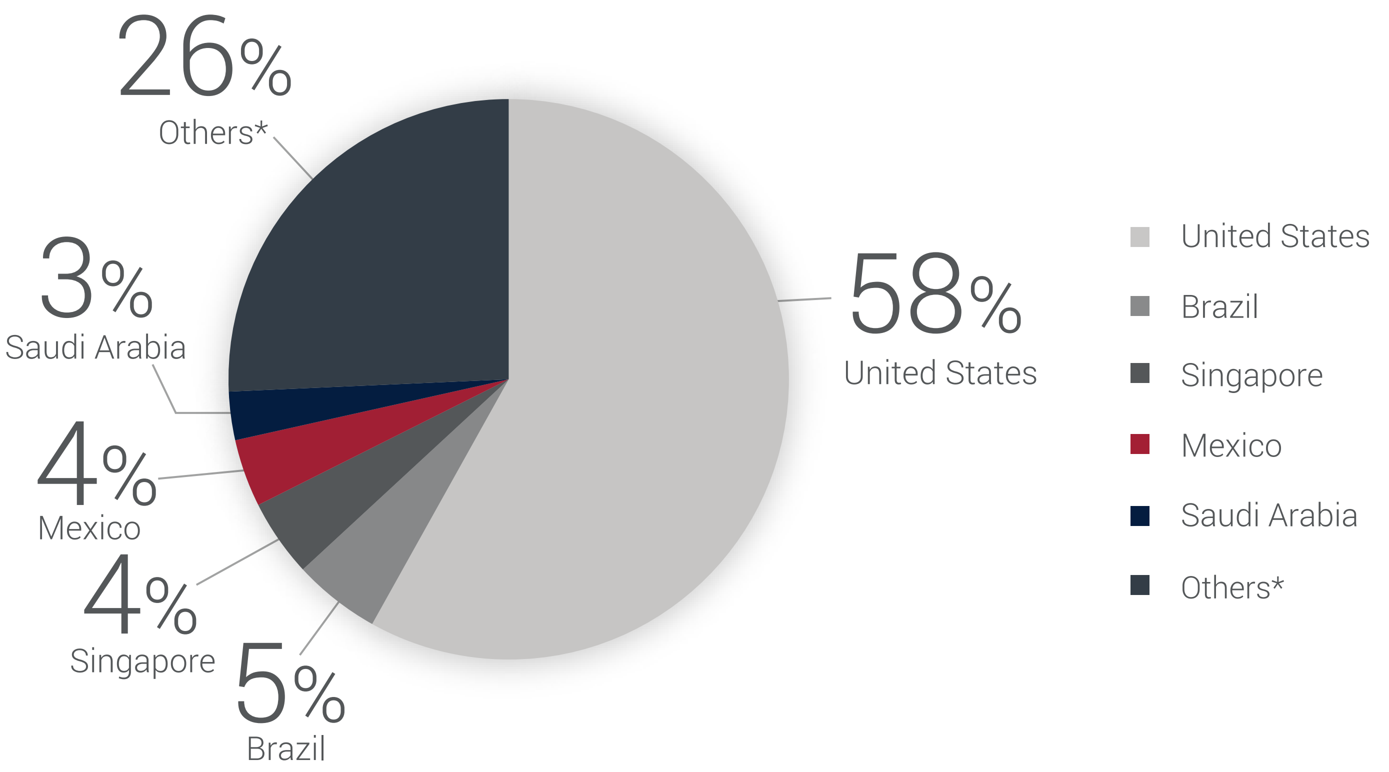
Others - includes E-commerce, Education, Electronics / Hardware, Energy, Industrial Goods, Media, Real Estate, Retail, Telecommunications and more.*

Participants by Job Function

Participants include entrepreneurs, intrapreneurs, individual contributors, and cross-functional teams. Representative job functions and titles include:

- CEO & Founder
- Chief Technical Officer
- CISO
- CTO
- Senior Principal Director
- Director of Enterprise Information Security
- Director of Emerging Technologies
- Director of Cloud Operations
- Associate Director, IT
- VP- Technology Officer
- Head of Risk Management
- Chief Technologist
- Global Security Manager
- Network Infrastructure Manager
- Security and Infrastructure Manager
- Cybersecurity Engineer
- Enterprise Solutions Architect
- Cloud Solution Architect
- Information Security Analyst

Participants by Region



Others - includes Australia, Cambodia, Canada, Colombia, Croatia, France, Germany, Hong Kong, India, Indonesia, Ireland, Italy, Japan, Malaysia, Peru, South Africa, Switzerland, United Kingdom and more.*

Representative Companies

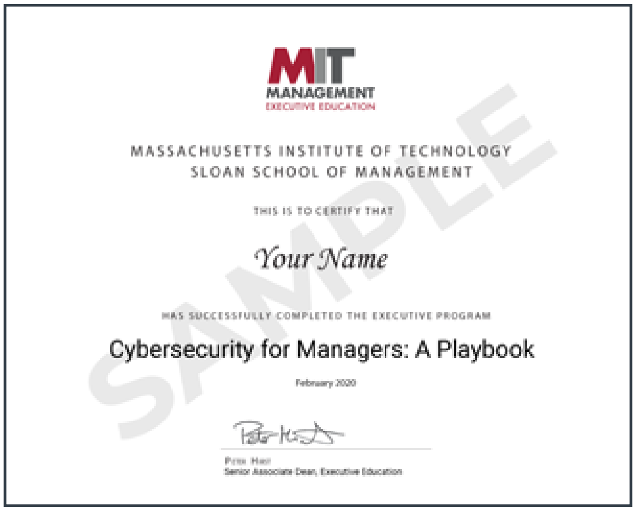
Participants include employees from companies like:

- Atos
- Australia and New Zealand Banking Group Limited
- Bank of America
- CISCO
- Citigroup Inc.
- FedEx
- GE
- Johnson & Johnson
- Microsoft
- National Bank of Cambodia
- Oracle Corporation
- Paypal
- Qatar Steel
- Singapore Telecommunications Limited
- Tech Mahindra Limited
- U.S Bank
- Walmart Inc.
- Wells Fargo

CERTIFICATE

Get a verified digital certificate of completion from MIT Sloan School of Management. This program also counts towards an MIT Sloan Executive Certificate.

Note: After successful completion of the program, your verified digital certificate will be emailed to you in the name you used when registering for the program. All certificate images are for illustrative purposes only and may be subject to change at the discretion of MIT Sloan. You may share your digital certificate on social media and in your professional bio.



MIT MANAGEMENT EXECUTIVE EDUCATION

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
SLOAN SCHOOL OF MANAGEMENT

THIS IS TO CERTIFY THAT

Your Name

HAS SUCCESSFULLY COMPLETED THE EXECUTIVE PROGRAM

Cybersecurity for Managers: A Playbook

February 2020

Peter Hirst
Senior Associate Dean, Executive Education

ABOUT MIT SLOAN SCHOOL OF MANAGEMENT

The MIT Sloan School of Management, located in Cambridge, Massachusetts, is part of the Massachusetts Institute of Technology. MIT has over 120,000 alumni in over 90 countries who have founded more than 30,000 companies. MIT's motto is "mens et manus," or "mind and hand," signifying the fusion of academic knowledge with practical purpose. The mission of the MIT Sloan School of Management is to develop principled, innovative leaders who improve the world and to generate ideas that advance management practice.

ABOUT EMERITUS

MIT Sloan Executive Education is collaborating with online education provider EMERITUS to deliver its executive programs through a dynamic, interactive, digital learning platform. By working with EMERITUS, MIT Sloan Executive Education brings its growing portfolio of courses online to address the evolving demands of executives. EMERITUS' approach to learning is based on a cohort-based design to maximize peer to peer sharing and includes live teaching with world-class faculty and hands-on project based learning. In the last year, more than 30,000 students from over 150 countries have benefited professionally from EMERITUS' courses.

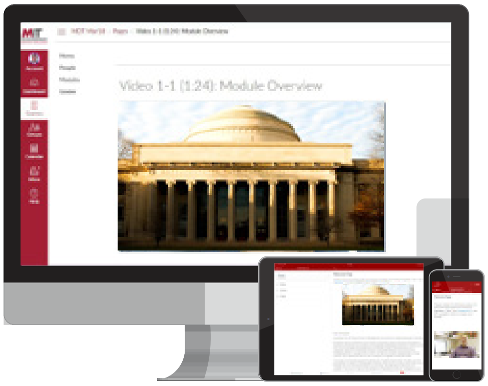
THE LEARNING EXPERIENCE

Our programs are designed to meet the needs of individual learning styles, while also leveraging the power of peer learning. This is achieved through a user-friendly learning platform that enables participants to easily navigate the program content to achieve learning objectives.

KEEPING IT REAL

Our pedagogical approach, designed to bring concepts to life, includes:

- Byte-sized learning elements
- Real-world application with the Playbook
- Peer learning discussions
- Active support from program Learning Facilitators



KEEPING IT CONVENIENT

Access to program content is flexible, available through multiple devices allowing working professionals to easily manage schedules and learn remotely — anytime, anywhere. Participants obtain access to learning materials via a modular approach, with new content released weekly.

KEEPING IT ENGAGING

Our online classroom enable participants to seamlessly interact with their peers and stay on track towards program completion — with culturally-enriching encounters along the way. Program modules consist of a variety of teaching instruments, including:

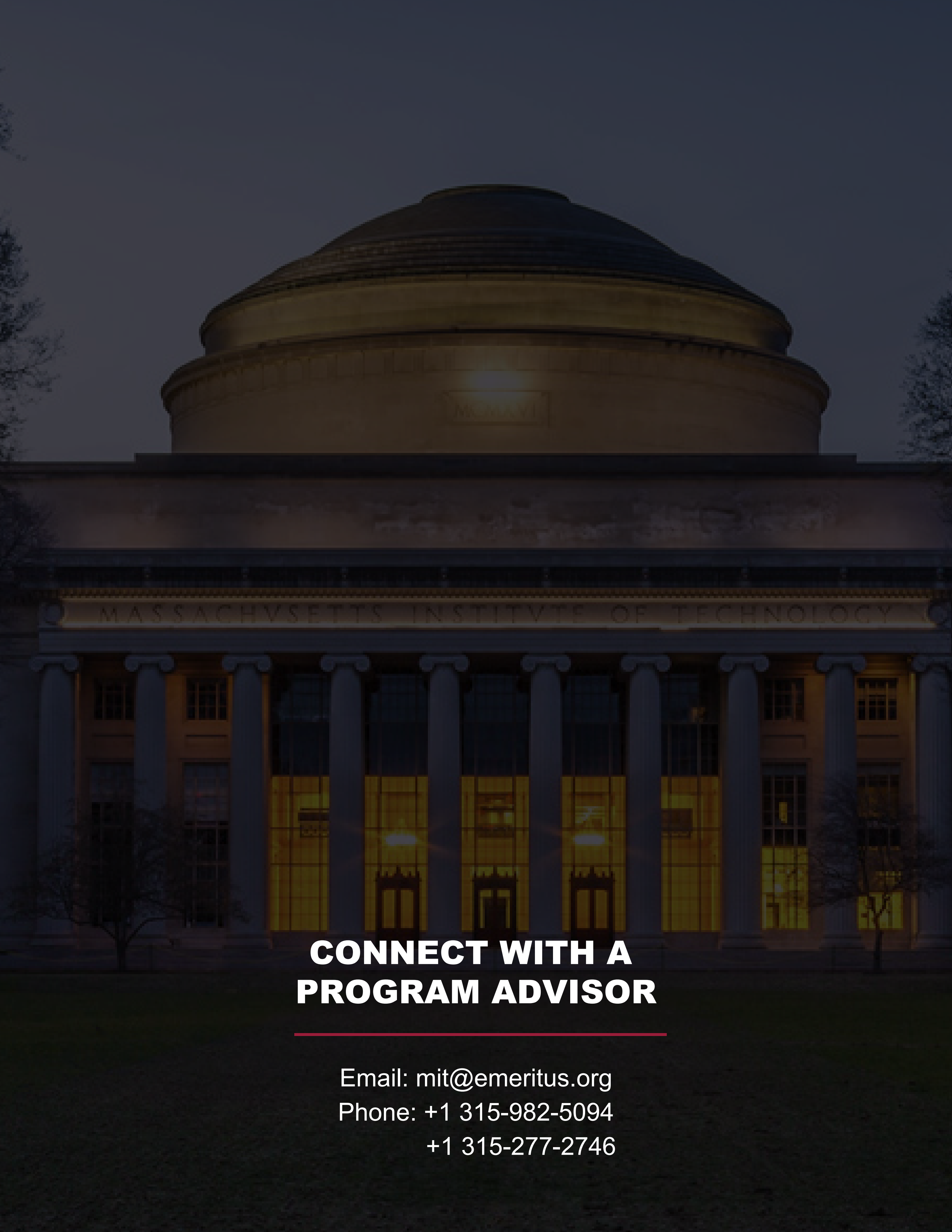
- Video lessons
- Moderated discussions
- Class materials: articles, cases
- Quizzes
- Surveys
- Learning journey support offered by a dedicated Learning Facilitator team
- Interactive cyber security simulation
- Office hours with program support team

Access Requirements

- Valid email address
- Microsoft Office suite
- PDF viewer to view all documents and presentations
- Computing device connected to the internet
- Latest browser version to access our learning platform

Other Requirements

Certain programs may require the usage of additional software, tools, or applications. Participants will be informed about these additional requirements at the registration stage or during program commencement. Our program advisors are also available to respond to any questions about these requirements.



CONNECT WITH A PROGRAM ADVISOR

Email: mit@emeritus.org
Phone: +1 315-982-5094
+1 315-277-2746