ONLINE MASTERS IN CYBERSECURITY MANAGEMENT

Tulane University
SCHOOL OF PROFESSIONAL ADVANCEMENT

Program Overview

The Online MPS in Cybersecurity Management program will provide you with critical knowledge and leadership skills specifically relevant to the cybersecurity industry. Additionally, you will gain hands-on skills from a variety of practical lab experiences in your technical courses. Learn from current practitioners how to tackle real-world cybersecurity challenges with IT solutions that are powerful, relevant and effective.

Our program will teach you how to:

- Identify security risks and known threats
- Formulate preventative security controls
- Articulate and champion business cases for security projects
- Implement a tailored, organizational cybersecurity posture
- Develop security budgets based on risk modeling
- Institutionalize security-relevant governance policy

Choose elective courses that lead to a choice of two optional in-demand concentrations:

- Homeland Security
- Emergency Operations

About SoPA

For more than 130 years, Tulane's School of Professional Advancement has helped working adults pursue higher education and advance their careers. In addition to campus-based programs, we now offer online programs of the same quality, taught by the same dedicated faculty. We've taken what makes Tulane one of the country's most respected institutions of higher education—and brought it all online.

- ✓ No GRE or GMAT required
- ✓ Complete in 16-24 months
- ✓ Full and part-time scheduling options
- ✓ 33 credits
- ✓ $1078 cost per credit*

* Some courses have lab fees of up to $150 per course to support the technology needed for high-quality virtual labs. These fees are always listed on the schedule of classes.

Sample Part-Time Course Schedule

TERM 1	TERM 2	TERM 3	TERM 4	TERM 5	TERM 6
Leadership and Management Principles for Cyber-security Professionals	Cyber Network and Telecommunications Security	IT Security Auditing and System Monitoring	Data and Database Security	Business Principles and IT Security Management	Enterprise Cybersecurity Management Capstone
Security and Cyber Threats for IT Managers	Cybersecurity Law and Policy	Cryptography	Wireless, Mobile and Cloud Security*	Cyber Threats and National Security*	

*elective

YOUR COURSEWORK INCLUDES:

Leadership and Management Principles for Cybersecurity Professionals
Cybersecurity management throughout an enterprise: Examine internal and external security threats against a network to learn how to document and advocate for cybersecurity spending, resource management and security governance development to protect an organization's critical information.

Security and Cyber Threats for IT Managers
Threat detection: Discover IT threats and current and evolving exploitation methods and vulnerabilities. Learn about attacks and attackers and analyze their motivation, purpose, types, and phases, considering threats from emergent technologies (such as Blockchain, IoT, and Quantum Computing).

Cyber Network and Telecommunications Security
Enterprise security of networks and telecommunications: Examine defense architecture, along with best practice implementations of security tools and solutions and methods and constructs for testing network security. Learn how to design a secure network.

Cybersecurity Law and Policy
Existing and evolving laws: Learn about agreements, legal decisions, regulation and compliance pertaining to cybersecurity and enterprise IT. Explore ethical considerations of cybersecurity practices, including social networking and privacy in the context of enterprise cybersecurity management.

IT Security Auditing and System Monitoring
Tools and methods to audit and monitor networks: Learn to audit, aggregate, analyze, report and respond from a cybersecurity management perspective. Participate in an in-depth system event, including intrusion, detection and prevention.

Cryptography
Ciphers, cryptology and encryption: Learn how cryptography is used to safeguard information and systems in an enterprise. Discover encryption, including access control, authentication, data application security, and virtual private networking. Learn about legal decisions and implications of encryption in the debate on privacy/civil liberties versus business and security/safety goals.

Data and Database Security
Database architecture: Learn the principles and methodologies of database design for security. Discover how to audit aggregate, analyze, report and respond from a cybersecurity management perspective. Learn how to secure data at rest, in transit and in use, against the context of noteworthy breaches.

Business Principles and IT Security Management
Business management and operational concepts: Learn to integrate and manage a cybersecurity operation within a greater organization. Consider core organizational management activities/business topics as they relate to IT Security, including cost/benefit analysis, procurement, making business cases for cybersecurity, IT budgeting and working with contractors and consultants.

Enterprise Cybersecurity Management Capstone
Apply all you've learned to affirm and display your mastery of Cybersecurity leadership and management.

SAMPLE ELECTIVE COURSES:

Cyber Incident Response and Forensics
Cyber incident response and investigation: Learn how to secure a cyber-incident scene, preserve digital evidence, establish and maintain chain of custody, conduct forensic analysis, and examine and review evidence.

Wireless, Mobile and Cloud Security
Architecture and security for Wireless, Mobile and Cloud Computing: Review network constructs as well as vulnerabilities and attack vectors. Learn how to implement and secure wireless networks, access and BYOD, including wireless security protocols, mobile IP communications, and cloud computing categories and services.

Software and Web Application Security
Software and web application vulnerabilities: Review the technologies, models, best implementation practices and known software and web application vulnerabilities. Discover how to plan, program, and manage secure applications through design and control interfaces.

Cyber Threats and National Security
Cyber threats to personal, organizational, economic and national security: Learn about the commercial and national security cross-threats posed by hackers. Discover the impact and relationship of digital espionage, cyber war, cyber terrorism, computer hacking, viruses, communications eavesdropping, forgery, and disruption to information flow to an enterprise.

Tulane University
SCHOOL OF PROFESSIONAL ADVANCEMENT