CYBERSECURITY TECHNOLOGY MANAGEMENT CERTIFICATE

The 3-course Cybersecurity Technology Management Certificate provides students with a background in both the technological and managerial skills needed to be an effective cybersecurity professional in today's IT enterprises.

Students will learn how to assess how organizational preparedness against cyber threats and how to manage their aftermath, including ensuring continuity of IT functions. Students also develop a strategy for designing and building cloud security architectures. An emphasis on ethical, legal, policy and regulatory concerns is embedded throughout the program.

Related Programs

Major

- Cybersecurity (BS) (https://catalog.luc.edu/undergraduate/arts-sciences/computer-science/cybersecurity-bs/)

Certificate

- Computer Science Certificate (https://catalog.luc.edu/undergraduate/continuing-professional-studies/computer-science-certificate/)
- Cybersecurity Certificate (https://catalog.luc.edu/graduate-professional/business/cybersecurity-certificate/)

Curriculum

Code	Title	Hours
Certificate Requirements		
CPST 381	Cybersecurity Governance	3
CPST 382	Cybersecurity Incident Response Management	3
CPST 383	Cloud Security Strategy and Architecture	3
Total Hours		**9**

Optional:

- CPST 265 Special Topics: Advanced Topics in Cybersecurity Technology Management: The optional course is included to address up-to-the-minute topics, such as emerging threats, insider threats, latest application delivery processes, and practices, etc.

Suggested Sequence of Courses

The School of Continuing and Professional Studies provides a high-touch advising model in order to incorporate the professional and educational outcomes of the student as well as any transfer credit accepted. In order to provide students with maximum flexibility in their education and because everyone's academic background will vary, advisors will work directly with students to determine an appropriate sequence of courses starting at admission into their respective program based on their needs and expected time to completion.

Learning Outcomes

- Explain the strategic importance of effective, interdisciplinary, and multifunctional enterprise information security governance and information security management program and its execution.
- Evaluate the effectiveness and potential application of multiple information security governance structures and information security management programs for variant enterprise scenarios with consideration for strategic, operational, ethical, social, environmental, and risk factors.
- Apply foundational knowledge of governance, risk, and compliance (GRC) concepts as they relate to legal, regulatory, and standards-based environments, such as HIPAA, FISMA, NERC, PCI DSS, GLBA, SOX, FERPA, COPPA, and others.