CYBERSECURITY CERTIFICATE

Never far from the day's headlines, data theft impacts business and consumers throughout our interconnected world. Due to a growing dependency on information security, businesses are hiring more cybersecurity professionals.

Quinlan graduate students have the unique opportunity to earn a certificate in cybersecurity from the highly ranked **University of Dallas** (UD) Gupta College of Business.

The online cybersecurity certificate is a graduate-level, five-course program that provides the foundational skills and knowledge for strategic cybersecurity management.

Related Programs

Certificate

- Cybersecurity Technology Management Certificate (https://catalog.luc.edu/undergraduate/continuing-professional-studies/cybersecurity-technology-management-certificate/)

Curriculum

Courses are scheduled to enable completion of the certificate in as fast as 4 trimesters, with students beginning the course sequence in fall or spring. Sessions meet once per week for 12-weeks on the following schedule. All courses are online.

Courses

The following courses are required for the certificate:

- TECH 5F70 - Foundations of Cybersecurity **or** CYBS 5F70 - Information Technologies and Management
- CYBS 6350 - Data Protection
- CYBS 6355 - Compliance and Legal Issues
- CYBS 7350 - Operational Cybersecurity Management
- CYBS 7357 - Network Security

More information can be found on the Quinlan School of Business (https://www.luc.edu/quinlan/academics/graduatecertificates/cybersecurity/) website.

Course Descriptions

TECH 5F70: Foundations of Cybersecurity (OR) CYBS 5F70: Information Technologies and Management (Pick one)

TECH 5F70: This course examines the global issues facing IT and Cybersecurity organizations today by providing an understanding of IT infrastructure, services, and technologies for competitiveness, efficiency, and effectiveness. Students investigate security threats faced by enterprises through the tenets of cybersecurity of confidentiality, integrity, availability, and governance.

CYBS 5F70: This course provides an introduction to the study of cybersecurity and the need to maintain confidentiality, integrity and availability of information. Students will be introduced to cyber laws and governance issues, risk management, security tools, security awareness and the ongoing responsibilities associated with maintaining a secure organization.

CYBS 6350: Data Protection

Provides a working knowledge of fundamental data protection techniques for protecting data at rest, data in motion, and data in processing. Techniques include encryption algorithms and systems (symmetric, asymmetric, standard, digital certificates, and hashes), Steganography, data masking, and data obfuscation. Examines access controls, availability, authentication, confidentiality, data integrity, and non-repudiation as well as defenses against DDOS and other data attacks. Security by diversity and security in depth are presented as fundamental requirements.

CYBS 6355: Compliance and Legal Issues

Examines legal, privacy, and compliance environments facing organizations globally. Students build an understanding of the complexities of security, compliance and legal obligations starting with a general foundation of laws and industry standards that apply across most organizations that handle sensitive data. Examination of industry verticals expand students' knowledge of particular federal and state regulatory and industry-based obligations. It also examines how security and compliance obligations can be used to establish the security, compliance, and risk management programs for an enterprise. Equivalent to TECH 6355.

CYBS 7350: Operational Cybersecurity Management

Focuses on developing skills relative to an understanding of the business risks that exist when proper cybersecurity access controls are not effectively implemented. Students will study breach cases and have the opportunity to interface with security experts to gain an in-depth understanding of current risks, threats, and vulnerabilities organizations face. Lab simulations will be completed and each lab will be analyzed for its meaning and purpose in increasing security knowledge. Students will create a cybersecurity breach report and as a team project create an access control plan with recommendations for overcoming or minimizing cyber breach situations through the use of proper controls, the control framework, lab experiences, and other resources explored in the course. Co-requisite: CYBS 6350. Equivalent to TECH 7350.

CYBS 7357: Network Security

Provides a comprehensive explanation of network security basics including how hackers access networks and the use of network security tools to provide countermeasures. Strategies for meeting the challenges from expanded network boundaries are developed through active hands-on exercises in networked lab environments. Prerequisite: CYBS 5F70 and CYBS 6350.

Suggested Sequence of Courses

The below sequence of courses is meant to be used as a suggested path for completing coursework. An individual student's completion of requirements depends on course offerings in a given term as well as the start term for a major or graduate study. Students should consult their advisor for assistance with course selection.

Fall Start

Trimester
Fall Start: Late August
Fall End: Mid November

- CYBS 5F70 - Information Technologies and Management

Trimester
Spring Start: Late January
Spring End: Mid April

- CYBS 6350 - Data Protection **and** CYBS 7350 - Operational Cybersecurity Management

Trimester
Summer Start: Early June
Summer End: Mid August

- CYBS 6355 - Compliance and Legal Issues

Trimester
Fall Start: Late August
Fall End: Mid November

- CYBS 7357 - Network Security

Spring Start

Trimester
Spring Start: Late January
Spring End: Mid April

- CYBS 5F70 - Information Technologies and Management

Trimester
Summer Start: Early June
Summer End: Mid August

- CYBS 6350 - Data Protection

Trimester
Fall Start: Late August
Fall End: Mid November

- CYBS 6355 - Compliance and Legal Issues **and** CYBS 7350 - Operational Cybersecurity Management

Trimester
Spring Start: Late January
Spring End: Mid April

- CYBS 7357 - Network Security

Earn Microcredentials

Upon successful completion of required coursework, students receive a verified University of Dallas microcredential (https://udallas.edu/minimasters/) in “Cyber Operations.”

Microcredentials demonstrate mastery of in-demand skills to potential future employers. They can be displayed with a special digital badge from the University of Dallas on your LinkedIn account and resume. Through Acclaim (https://www.credly.com/organizations/university-of-dallas/badges/), your accomplishment can be verified by employers and hiring managers.