MASTER OF SCIENCE IN CYBERSECURITY

The Master of Science in Cybersecurity program provides a comprehensive understanding of cybersecurity methods, approaches, and concepts. It covers various cybersecurity techniques and continuously updates its content to address emerging issues and management solutions. The program explores cryptographic mechanisms and their application in securing computer systems and networks. It is designed for individuals with a solid foundation in information and communication technologies.

The program also covers the nature, scope, and significance of cybersecurity, justifying and exploring critical concepts. It examines cybersecurity threats and the technological and procedural mechanisms to mitigate them. The role of cryptography in ensuring security, including the use of algorithms in security programs, is discussed. The program also highlights the crucial support function of management and the role of cryptography.

Objectives and Methodology

The goals that the Master of Science in Cybersecurity aims to achieve are:

- Equip students with practical and applied skills to address the evolving demands of the cybersecurity field.
- Enhance proficiency in the latest tools, techniques, strategies, and technologies relevant to cybersecurity.
- Foster critical thinking abilities in analyzing how organizations manage security.
- Provide direct access to industry professionals with specialized expertise in crucial cybersecurity areas.
- Offer hands-on experience through real-world case studies that reflect contemporary challenges in the field.

Career Opportunities

The widespread global adoption of data management and production, facilitated by information technology, has made it increasingly critical for professionals to ensure cybersecurity in public and private institutions and companies, regardless of their size.

The professional profiles that are increasingly in demand and to which St. Thomas University is responding with the Master's program in Cybersecurity are:

Cybersecurity Expert, Data Protection Designer, Chief Information Security Officer, Chief Security Officer, Security Administrator, Security Architect, Security Engineer, Security Analyst, Ethical Hacker, Security Developer, General Data Protection Regulator, Digital Forensic Analyst, Data Protection Officer, and ICT Security Manager.

Curricular Program (36 CH)

A. Core Courses (27 CH)

COM 500 - Introduction to Cybersecurity
COM 505 - Cybersecurity Policy
COM 510 - Cyber Threat Intelligence
COM 515 - Cybersecurity Architecture
COM 520 - Fundamental Security Management and Governance
COM 600 - Applied Cryptography
COM 605 - Network and Infrastructure Security
COM 610 - Software and Application Security
COM 615 - Cybersecurity Research Methods

B. Core Electives (6 CH). Select two of the following four courses:

COM 517 - Cloud Security
COM 518 - Mobile Security
COM 519 - Wireless Security
COM 620 - Industrial Control Systems Security

C. Research and Master's Thesis (3 CH)

COM 690 - Master's Thesis