MASTER OF SCIENCE IN CYBERSECURITY

The Master of Science in Cybersecurity is structured to impart a thorough understanding of Cybersecurity methods, approaches, and concepts. The program focuses on a wide range of cybersecurity techniques and is constantly updated to address issues and how the organization's management solves these issues. Cryptographic mechanisms and their application on how to secure computer systems and networks are explored. The program is for those with a good general knowledge of information and communication technologies. Cybersecurity's nature, scope, and importance are covered, and critical concepts are justified and explored. Cybersecurity threats and the technological and procedural mechanisms employed will be examined. The role of cryptography in ensuring security, including how algorithms play a part in enabling security programs, will also be addressed. The critical support function performed by management and why the use of cryptographic functions depends on it is identified. The need for security management in an organization is explained, as well as its main elements introduced, including the critical role played by risk management, the importance of standardized security management, and the concept of compliance will be presented.

OBJECTIVES AND METHODOLOGY

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

- have students acquire practical and applied skills to meet current and emerging needs in the field of Cybersecurity
- master the latest and most relevant tools, techniques, strategies, and technologies
- develop the ability to think critically about how organizations manage security
- have direct access to industry professionals with specific expertise in key areas of cybersecurity
- gain experience working with real-world case studies that reflect new and current challenges

JOB OPPORTUNITIES

The massive global use of data management and production with information technology has made it increasingly critical for professionals capable of ensuring cybersecurity in public and private institutions and companies, whether large or small. 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 Design; Chief Information Security Officer; Chief Information 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; ICT Security Manager.

CURRICULAR PROGRAM

COM/500 - Introduction to Cybersecurity
COM/505 - Cybersecurity Policy
COM/510 - Critical Infrastructure Cybersecurity
COM/515 - Cyber Threat intelligence
COM/520 - Cybersecurity Architecture
COM/545 - Fundamentals Security Management and Governance
COM/550 - Advanced Security Management and Governance
COM/565 - Cybercrime
COM/585 - Applied Cryptography
COM/610 - Fundamentals Network and Infrastructure Security
COM/615 - Advanced Network and Infrastructure Security
COM/620 - Network and Host Forensics
COM/645 - Computer Systems Security
COM/660 - Fundamentals Software and Application Security
COM/665 - Advanced Software and Application Security
COM/675 - Safety and Behavior Change
COM/705 - Information Privacy
COM/850 - Cybersecurity Research Methods
COM/900 - Master Thesis or Capstone Project