MASTER OF SCIENCE IN CYBERSECURITY

WHY STUDY MASTER OF SCIENCE IN CYBERSECURITY

Our Master of Science in Cybersecurity has been carefully designed to develop qualified and skilled cybersecurity professionals. The programme covers cybersecurity from governance and policy to penetration testing and digital forensics. The programme builds the knowledge and skills to design, develop, defend and manage secure systems. The programme offers a wide range of learning opportunities in a stimulating learning environment. Additionally, the teaching materials, lectures, seminars, research, case studies and labs in our programme are informed by world-class research in AI and cybersecurity being undertaken at BUiD, in collaboration with experts holding globally-recognised industry-standard certifications.

CAREER PROSPECTS

Graduates can enter a range of careers in various sectors, including oil and gas, hospitality, energy, transportation, retail, manufacturing, defence, aviation, ICT, telecommunications, and banking/financial industries. They can work as cybersecurity managers, security engineers/architects, information security analysts, cybersecurity consultants, information security officers, digital forensic investigators, ethical hackers/penetration testers, threat hunters/malware analysts, and incident response specialists. Alternatively, graduates can pursue further studies by undertaking a PhD, which will pave the way for a research career in academia or industry.

ENTRY REQUIREMENTS

A relevant Bachelor's degree equivalent to an Upper Second Class or with a Good GPA (3.0 or above on a 4.0 scale or its equivalent) from an accredited university.
English Language proficiency is required equivalent to UAE Ministry of Education EmSAT score of 1400 or TOEFL score of 79 iBT or IELTS 6.0.

PROGRAMME STRUCTURE

Module title	Credits
Cybersecurity Science and Applications	3
Network Security	3
Cyber Threat Intelligence and Analysis	3
Cryptography and Information Security	3
Cybersecurity Governance, Risk Management, and Compliance	3
Informatics Research Methods	3
Elective modules: students have to choose TWO modules (subject to timetabling)	
Penetration Testing and Vulnerability Assessment	3
Digital Forensics and Incident Investigation	3
Cloud Security and Virtualization	3
Mobile Security and IoT Security	3
Selected Topics in Cybersecurity	3
Secure Software Development	3
Knowledge Management	3
Data Mining and Exploration	3
Dissertation	6
Total Credits	30