

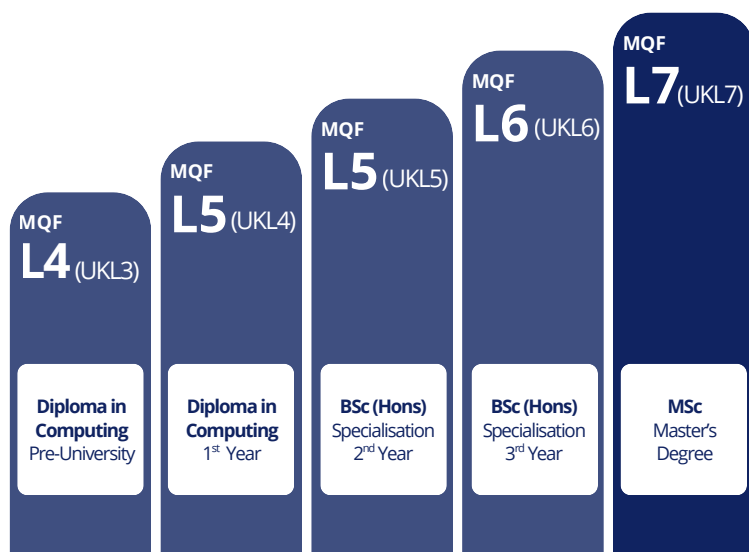
# MSc Cyber Security

## Master's Degree

The exponential increase in mobile devices, converged applications and Cloud Technologies, including initiatives such as Bring your Own Device (BYOD) / Choose Your Own Device (CYOD) and the advent of digital information technologies, has increased the proliferation of threats in our cyber environment. Cyberspace is constantly increasing its size almost linearly to its value, implementing cyber security as a global response to the challenges posed by constantly evolving systems that are harder to secure.

The MSc Cyber Security seeks to address the increasing demand for related domains in academic qualifications and projections for an increased shortage of professionals in the industry. The course has been designed by a team of leading experts, researchers and trainers in the field and gives the opportunity to the students to be exposed to cutting-edge technologies, tools and techniques in cyber exploitation and defence.

The diverse skillset around management of security as delivered on the course will equip students with a meaningful knowledge and relevant experience to excel in their career prospects.



### MSc Cyber Security

UK L7 - MQF L7

#### Credits

180 CATS - 90 ECTS

#### Awarding Body

University of Wolverhampton



#### Study Mode & Duration

Full-Time: One year

Part-Time: Two years

#### Assessments

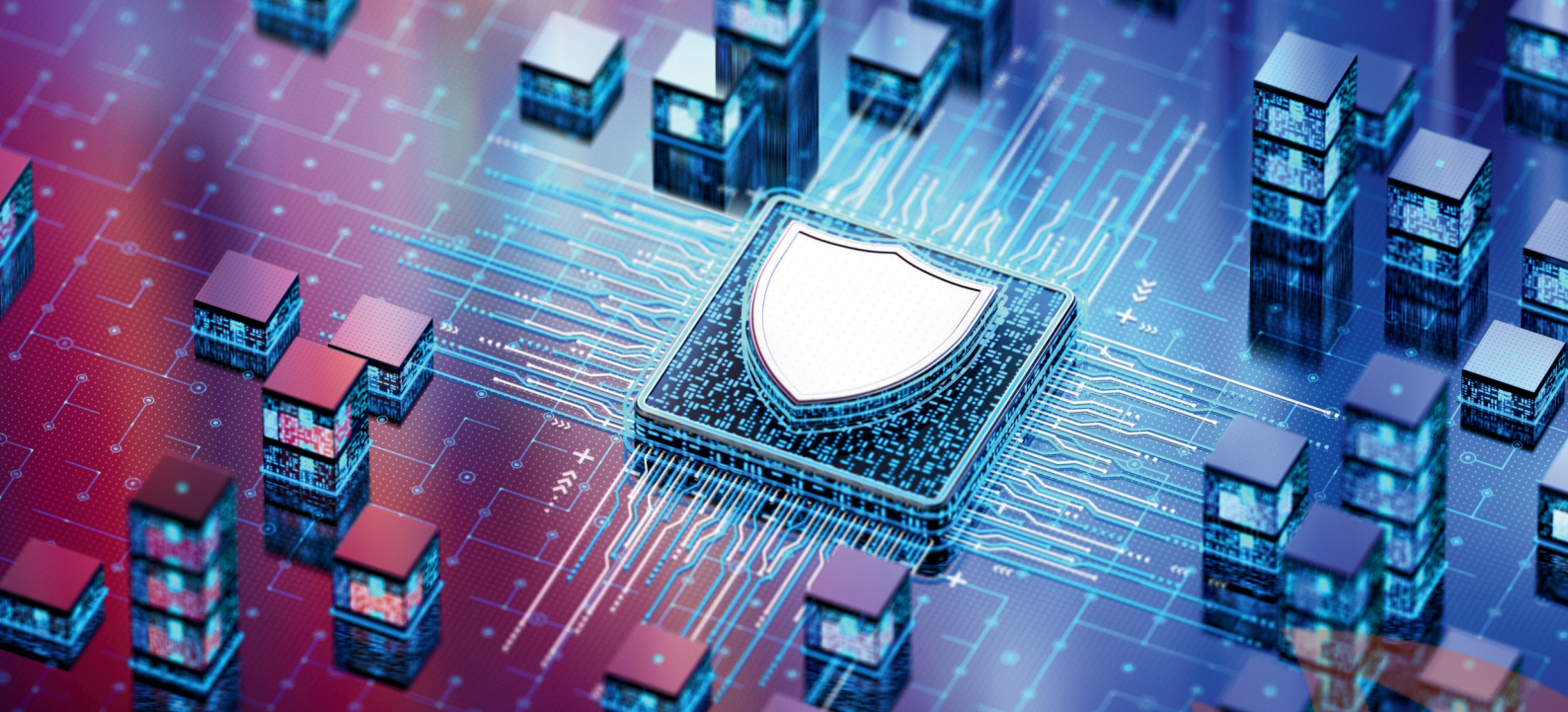
Examinations and coursework assignments

#### Entry Requirements

- Recognised undergraduate degree in a related field AND
- English language certification such as O Level or IELTS 6.5 with a minimum of 6.0 in each area or equivalent

Relevant work experience is considered





## MSc Cyber Security

### Ethical Hacking

Gain in-depth knowledge of penetration testing and vulnerability assessment, exploring offensive security with advanced tools and techniques. Learn to identify system weaknesses lawfully, applying skills across networks, operating systems, and human behaviour. Develop practical expertise in ethical hacking within a controlled, professional, and research-informed environment.

### Incident Management and Response

Learn the full lifecycle of incident response, from building a CERT team to forensic investigation and expert testimony. Gain hands-on experience with digital forensics tools, network analysis, and emerging threats. Understand relevant laws, ethical responsibilities, and strategies for managing incidents effectively.

### Proactive Network Defence

Study methods and tools for preventing cyber attacks and reducing detection time. Learn how to design secure networks, addressing strategic, tactical, and operational defence measures. Develop skills to adapt to evolving threats and improve the effectiveness of organisational security controls.

### Information Assurance

Explore frameworks, standards, and strategies for protecting information assets. Learn to align governance, risk, and compliance practices with legal and regulatory requirements. Understand multi-disciplinary processes that safeguard data within modern organisations and address evolving information governance challenges.

### Internet of Things Security

Examine IoT devices, applications, and underpinning technologies such as wireless sensor networks, Wi-Fi, and embedded systems. Identify emerging IoT threats and plan effective mitigation techniques. Gain experience securing interconnected devices, from sensors to autonomous systems, within diverse and complex environments.

### Research Methods in Computing

Develop the skills to design and conduct postgraduate research in computing. Explore research methodologies, professional conduct, and the legal, social, and ethical implications of your work, following BCS guidelines. Prepare to undertake substantial, academically rigorous research projects.

### MSc Project Cyber Security (60 credits)

Undertake a major project integrating technical, analytical, and managerial skills. Work under academic supervision to develop an approved idea into a practical artefact that could take various forms such as a set of technical documents or a framework. Follow ethical guidelines whilst producing work that reflects your cyber security expertise.