Cyber Security TM256 - AL person specification

Presentation pattern: B presentation - annually February to August

Module description

The National Cybersecurity Strategy, 2016 and further consultations by DCMS have clearly identified:

- That cyber-attacks remain a threat to the UK economic well-being and that cybersecurity skills shortage is one of the challenges likely to drive UK security priorities;
- The need to invest in the ability to detect analyse and defend against cyber-attacks in the government and private sectors.

It is in this context, the new BSc degree in Cybersecurity is being conceived and designed. This Cyber Security module is one of the two core modules designed as part of the qualification. The main references for the module are the Cybersecurity Body of Knowledge (CyBOK) and the (Skills Framework for the Information Age) SFIA skills framework. These frameworks describe the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles.

The UK National Cyber Security Centre has developed a body of knowledge for cyber security (https://www.cybok.org), which identifies three high-level domains for the field:

1. systems security;
2. infrastructure security;
3. software & platform security.

Together with two cross cutting aspects:

1. human, organisational & regulatory,
2. attacks & defences.

The module is organised into five blocks:

- Block 1: *Concepts of Cyber Security*
- Block 2: *Systems Security*
- Block 3: *Infrastructure, Host and Application Security*
- Block 4: *Security operations and Incident Management*

- Block 5: *Fundamentals of Digital Forensics*

Lecturers teaching on this Module are expected to keep up to date with cyber security developments that emerge during the lifetime of the TM256 module.

Person specification

The person specification for this course should be read in conjunction with the generic person specification for an associate lecturer at The Open University. As well as meeting all the requirements set out in the generic person specification, you should have:

- an undergraduate degree or equivalent professional experience in cyber security, computing, ICT or cyber security related field;
- Experience of teaching, working and/or research in one or more of the following: systems security, cryptography, infrastructure, host & applications security, security operations and incident management and fundamentals of digital forensics;
- An understanding of the underlying social, professional, ethical and legal issues relevant to cyber security;
- Enthusiasm for developing students' knowledge & practice in cyber security and in setting this in the context of our modern world.

Ideally, candidates would additionally have:

- Experience of using cyber security applications and open source based tools e.g. Kali Linux;
- Experience of using virtual environments e.g. VirtualBox and Netlab+.
- Experience of teaching cyber security at undergraduate and/or postgraduate level;
- Industry certifications (e.g. CASP+, CEH, CISSP, CRTSA, CyberOps).

Additional information

- In addition to marking three tutor-marked assignments (TMAs) and an Exam, you will also have to actively monitor student engagement on four interactive quizzes and respond to student queries about the quizzes;
- The minimum computer specification for OU students is insufficient for electronic marking of assignments. We recommend a large monitor (*at-least* 17-inch) or a second screen for marking purposes. You may need significantly more free disk space than is recommended for students.

Credits awarded to the student for the successful completion of a module:	30
Number of assignments submitted by the student:	3
Method of submission for assignments:	2
Level of ICT requirements:	2
Number of students likely to be in a standard group:	20
Salary band:	3
Estimated number of hours teaching per week:	3.5 hours