Department of Computer Science

# CS3609 Cybersecurity

## Undergraduate Study Guide for 2023/24

## TABLE OF CONTENTS

## MODULE DETAILS

| | | |
|---|---|---|
| **Module Leader** | Nura Abubakar | |
| **Department** | Computer Science | |
| **Credits** | 20 | |
| **Other staff** | Panos Louvieris, David Bell, Ferdoos Hossein | |
| **Contact and private study time** | Lectures<br>Labs/Seminars<br>Independent Study Hours (Coursework Study & General Study)<br>**Total** | 12 hours<br>18 hours<br>170 hours<br>**200 hours** |
| **Assessment** | **Method:**<br>**Coursework:**<br>**Examination:** | Single assessment element separated into two un-weighted tasks<br>Task 1 – Threshold coursework<br>Task 2 – Unseen examination to determine final module grade |

## ACCESS TO SUPPORT MATERIAL AND ADDITIONAL INFORMATION

The majority of the teaching, learning and support material is provided electronically via the University's Brightspace system. Note that the details provided in this study guide are based on the formal module syllabus for this module which sets out the agreed content, learning outcomes, assessment and teaching methods. Module syllabus and scheme of studies documents for your programme of study can be found by on the University's Quality Assurance web pages.

## INTRODUCTION/AIMS/BACKGROUND

**The aim of this module is to:** *Develop the competencies and skills sets required for delivering Cybersecurity solutions in practice*. Cybersecurity is a major concern for governments, companies, organisations and citizens alike. Cyber-attacks undermine our ability to conduct business in the global digital economy. Cybersecurity competencies are required to protect digital assets and minimise the threat, disruption and costs associated with attacks. An understanding of the theoretical and practical fundamentals of cybersecurity is necessary to prevent and defend against potential security breaches (e.g., Exfiltration APT, Ransomware, etc.). This module covers the essentials of cybersecurity commensurate with the BCS accreditation guidelines. Further, the module content complies with the (ICS)$^2$ organisation's topics required for CISSP (Certified Information Systems Security Certification) certification[1]. The roadmap for the module is illustrated in Figure 1 below.

[1] https://www.isc2.org/Certifications/CISSP

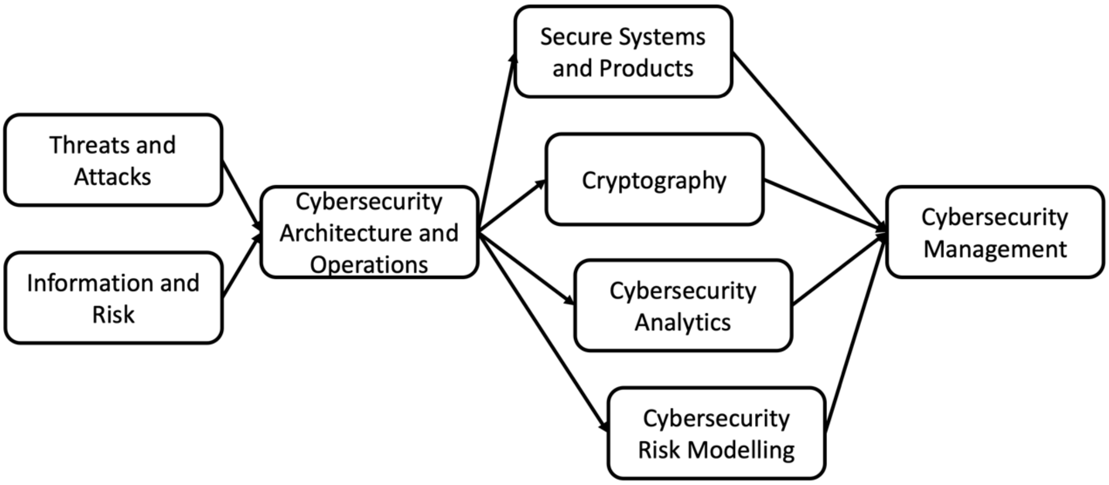

**Figure 1. CS3609 Cybersecurity Roadmap**

## Learning Outcomes

Whatever module or programme of study you are studying at Brunel University London, there are learning outcomes (LO) that you must meet/achieve in order to be awarded the credits which comprise the module and programme of study. In order to get a pass grade (D- or above) in this module, you must meet these learning outcomes below, that is, you must demonstrate ability to:

LO1: Demonstrate an understanding of the fundamental concepts and theories of Cybersecurity.

LO2: Demonstrate evidence of critical thinking, analysis, synthesise and evaluation in the design and formulation of Cybersecurity solutions.

LO3: Select relevant Cybersecurity tools and techniques and show how they can be effectively applied to solve real-world problems in the Cyberspace.

## Method of Teaching

***Lectures***: After an initial lecture to introduce the module, there will be eight further lectures in Term 1 (the schedule is set out in the next section). Each of these lectures will cover one Cybersecurity topic. There will then be a revision lecture at the end of term.

***Seminars/Labs***: The two-hour seminars/labs provide a small-group forum in which you can discuss/debate the topics assigned, using structured seminar/lab sheets that will be given to you in advance, and apply your skills in research, evaluation, synthesis and effective communication. Topics presented in the lectures will be the focus of the seminars/labs, allowing you to research and explore them in more detail. These topics are subject to assessment through coursework during Term 1 and examination at the end of the year, so preparation for and participation in the seminars/labs will help to prepare you for both assessments. The schedule for the seminars/labs is set out in Lecture Seminar/Lab Programme section below. The groups will be set up and published on Blackboard at the start of Term 1 and will be visible on your individual timetables. All the seminars/labs will be facilitated by a member of the teaching team.

***General Study***: The general study activity will allow you to (a) investigate and analyse the topics in-depth thorough review of appropriate literature/materials, (b) summarise and synthesize complex material, (c) relate the material to practice, understanding its relevance to and impact of society and the economy, and (d) curate the resources that you use so that you have a body of material that prepares you for the assessment.

## Lecture/Seminar/Lab Programme

This module has been scheduled to run during Term 1 and the lectures are scheduled as follows:

Term 1

| Week<br>Lec/Lab/Sem Dates | Lecture Topic<br>(1-hour session) | Lecturer | Seminars/Labs<br>(2-hour block session) |
|---|---|---|---|
| **Week 1**<br>*21 Sep* | **Introduction to Cybersecurity:** Context, Concepts and Roadmap | ←NA | No |
| **Week 2**<br>*28 Sep* | **Information and Risk:** Models including Confidentiality, Integrity and Availability (CIA); concepts such as probability, consequence, harm, risk identification, assessment and mitigation; as well as, the relationship between information and system risk. | ←PL | No |
| **Week 3**<br>*5 Oct* | No | PL→ | **Information and Risk Seminar (Case study exercise)**<br>Yes – Groups, Seminar |
| **Week 4**<br>*12/13 Oct* | **Threats and Attacks:** Threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities. | ←FH→ | **Threats and Attacks Lab**<br>Yes, Practical Lab |
| **Week 5**<br>*19/20 Oct* | **Secure Systems and Products:** The concepts of design, defensive programming and testing and their application to building robust, resilient systems that are fit for purpose. | ←NA→ | **Secure systems and products Lab**<br>Yes – Group Practical, Lab |
| **Week 6**<br>*26/27 Oct* | **Cybersecurity Architecture and Operations:** Physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance. | ←NA→ | **Cybersecurity architecture and operations Seminar**<br>Yes – Group Seminar |
| **Week 7** | **Reading Week** | **n/a** | **n/a** |
| **Week 8**<br>*9/10 Nov* | **Cybersecurity Analytics:** Application of intelligent cybersecurity analytics for the detection, prevention and prediction of cyber-attacks. AI, ML and statistical techniques for intrusion detection, anomaly detection and multi-source fusion. | ←FH→ | **Cybersecurity Analytics Lab**<br>Yes – Group Practical, Individual basis (in front of pc with R), Lab |
| **Week 9**<br>*16/17 Nov* | **Cryptography:** Fundamental cryptographic approaches, such as public-key encryption, digital signatures, pseudo-random number generation, and basic protocols and their computational complexity requirements. | ←DB→ | **Cryptography Lab**<br>Yes – Group Practical, Lab |
| **Week 10**<br>*23 Nov* | **Cybersecurity Management:** Understanding the personal, organisational and legal/regulatory/privacy context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cybersecurity is implemented | ←PL | No |
| **Week 11**<br>*30 Nov/1 Dec* | **Cybersecurity Risk Modelling:** examine system abstractions and the profiling of attackers (including goals and approaches). Resulting models catalogue risk/threats before simulation in agent models. | ←DB<br>PL→ | **Cybersecurity management**<br>Yes – Groups, Seminars |
| **Week 12**<br>*7 Dec* | **Revision** | ←NA | No |

**+ 2 REVISION Lecture/Drop-In Sessions (T2 and T3)**

**Key:**

Arrows ← and → depict lecturer/lab/sem responsibility.

| | |
|---|---|
| NA | Nura Abubakar |
| PL | Panos Louvieris |
| DB | David Bell |
| FH | Ferdoos Hossein |

**Please note:** Week 7 in Term 1 and week 22 in Term 2 are weeks during which there are no scheduled lectures, labs, or tutorials. Week 17 is the first week back after the Christmas break.

## Reading List

### Core reading list

Four books have been identified as suitable core reading to complement the Cybersecurity topics covered in this module and are available as eBooks from the Brunel University London Library. The most comprehensive book is the CISSP Study Guide (Stewart et al., 2018). Students might also wish to look at Security in Computing (Pfleeger et al., 2015) which has a slightly more technical perspective, or, the Kim and Solomon (2018) book, which is more up to date in terms of including Cybersecurity for IoTs. A good general reference and overview of Cybersecurity is the National Cyber Security Centre's CYBOK eBook (2019). It provides a good entry point for further supplementary reading. Additional resources will also be referred to via Blackboard on the relevant seminar/lab sheets where necessary, providing a starting point for your research to prepare for the seminars/labs.

- Stewart, J. M. et al. 2018. CISSP Study Guide. 8th ed. Indianapolis: Sybex.
- Kim, D. and Solomon, M.G. 2018. Fundamentals of Information Systems Security. 3rd ed. JBL: Burlington.
- Pfleeger, C. P. et al. 2015. Security in Computing. 5th ed. New Jersey: Prentice Hall.
- Rashid A., Chivers, H. et a.l 2019. CyBOK: The Cyber Security Body of Knowledge. Ver.1.NCSC. © Crown Copyright, The National Cyber Security Centre. Accessible online from: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

### Supplementary Reading

Please note that there is a wealth of material, much of it freely available on the web or in the library. The above are suggestions but you are encouraged to search for and make use of other sources. For example, the National Cyber Security Strategy 2016 to 2021 and other materials available from the National Cyber Security Centre:

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- https://www.ncsc.gov.uk/

It is important that you learn to become self-reliant and able to access and assimilate material for yourself. Many of the topics necessary for this project will not be covered by lectures. Therefore, you will need to work through the exercises and guidance material provided in labs, via Blackboard and from your own investigations.

## Assessment

This module is assessed by a single assessment element separated into two unweighted tasks. The assessment addresses all learning outcomes for this module.

**Task 1) Threshold Coursework**
**Design Project Study with a Reflective Essay (2,000 words)**

The maximum grade/mark you can achieve for this assessment is D-/40%, which demonstrates performance in the module at threshold level. Passing the threshold coursework means that you have passed the module overall.

The assessment of Task 1, which will be undertaken in Term 1, will be confirmed by the Panel of Examiners and, if necessary, the Board of Examiners will offer a reassessment of Task 1 in Term 2 by written submission and viva voce, subject to the re-assessment limitations of SR2. Prior to re-assessment, they will be given formative feedback to help them to undertake remedial work towards meeting the standard.

**A student who fails to achieve grade D- in Task 1 at both the first and second attempt will not be eligible for any further assessment/re-assessment in the module (including Task 2).**

Students who have been confirmed as passing Task 1, at either first or second attempt, will also take Task 2:

**Task 2) Unseen Examination (3 hour)**

The examination will assess only those students who have passed Task 1 at either the first or second attempt and will test the full grade range up to A*. Students who achieve D- grade or better in the examination will be awarded the examination grade for the module.

### Late Coursework

The clear expectation is that you will submit your coursework by the submission deadline stated in the study guide. In line with the University's policy on the late submission of coursework (revised in July 2016), coursework submitted up to 48 hours late will be accepted but capped at a threshold pass (D- for undergraduate or C- for postgraduate). Work submitted over 48 hours after the stated deadline will be graded as Non-Submission (NS), without accepted Extenuating Circumstances. Work submitted more than 5 days late will not normally be accepted.

### Deliverables and Feedback – Important Dates

You should prepare and submit all coursework according to the instructions in the relevant assessment brief. You should make sure that you are fully aware of the University's policy on plagiarism and collusion. You should also be aware that you *cannot* later claim that you did not know the rules and regulations as you must make yourself familiar with them. If you cannot complete any work on time, you should look at the Department's instructions on what to do. The Department policy is that all coursework must be submitted electronically via the WISEflow system. Please navigate to the Brightspace pages for this module for further details. You will get feedback on your performance via WISEflow for this module. If do not receive your feedback by the given date, you should first contact the module leader. If it proves necessary, you should also contact the Director of Undergraduate Studies.

**The important dates:**

In the table below, the key dates and tasks associated with the assessment for the module are set out.

| Task | Assignment Title | Available on Brightspace | Submission Deadline | Feedback Due | Weighting |
|---|---|---|---|---|---|
| T1 | Coursework | 27.10.2023 | 24.11.2023<br>11:00 am<br>UK time | 15.12.2023 | This is a Threshold Coursework |

**Note:** all deadlines are at 11.00 a.m. UK time on the stated date (e.g., if the deadline is 1 February, it means the deadline is 11 a.m. UK time on 1 February).

### Expectations of Artificial Intelligence Use

In this module, you can use generative AI tools such as ChatGPT, Bing AI, or Bard to complement you learning by using them as supplementary resources. For instance, you can use AI tools to understand the MITRE ATT&CK Framework (MAF), Cryptography, and other complex topics. However, you must use AI with caution and responsibility in this module. You should be mindful of the potential for bias and inaccuracies in the generated content due to the limitations of the training data. You should never present AI-generated work as your own, which could lead to academic misconduct. Additionally, you should take measures to ensure that any personal data or sensitive information exposed to AI tools is adequately protected to prevent potential security breaches that could compromise cybersecurity. This module's ethical and responsible use of generative AI tools can be a valuable asset, but it must follow strict guidelines and academic integrity standards.

### Additional Vital Information

The College Student Handbook can be found on the University’s web pages. The handbook is a useful source of information for all aspects of your studies, including procedures of how to inform us of problems you are facing with your studies, how to apply for an extension to your coursework, plagiarism, house style for assignments, joint and group work submissions and other important matters.  The Department assumes that you familiarise yourself with this information, so you will need to look at these pages carefully at various times throughout your studies.  The Department also operates within the rules and regulations of the University more generally, and you should also look at what are known as 'Senate Regulations’ on the University’s web pages. These policies and procedures might change from one academic year to another, and it is in your interest to review them on an on-going basis.