Digital & Technology Solutions Professional: Cyber Security unit summaries

Year 1: Trimester 1

Digital Technology in Organisations & Society (15 credits)

Brief Summary: Businesses today operate in a dynamic, complex and highly integrated digital environment. This unit will challenge students to critically evaluate the impact of digital technology on contemporary businesses and their wider community. The unit will cover issues from the perspective of a simple business to the global business community touching on topics such as ethics and legal issues.

Indicative Content: The topics of the unit will include the following: Overview of contemporary digital technologies and their integration into business processes, business-technology alignment, phenomenon of digital transformation and its implications for businesses, organisation's culture and digital technologies, societal and environmental implications of digital technologies, Freeman's Stakeholder theory, Elkington's Triple Bottom Line, etc. and ethical and legal issues of digital technologies.

Introduction to Programming (30 credits)

Brief Summary: This unit introduces computer programming in a high-level programming language, developing your skills in problem-solving, program design, solution implementation and testing. You will learn fundamental programming principles, and how you can combine standard techniques to solve simple problems using computer software. You will gain practical experience in developing software using industry-standard programming tools in a variety of scenarios.

Indicative Content: The unit will introduce the basics of computer programming, using a contemporary programming language (e.g., Java/Python/C#). Students will use an industry-standard development environment and associated tools to create programs that help solve simple problems. The unit will introduce students to fundamental programming techniques (e.g., use of variables, data types, sequencing, selection, and iteration), along with basic techniques for structuring programmes (e.g., functions, classes, object orientation). Students will complete a variety of practical exercises providing experience of problem solving, software design, implementation, testing and debugging.

Year 1: Trimester 2

Database Fundamentals (15 credits)

Brief Summary: This unit introduces learners to the use of the relational model to structure data for efficient storage and retrieval. Learners will gain practical experience in the construction and usage of databases in an industry-standard database management system.

Indicative Content: Understanding the relational model and the client/server model for databases; interacting with relational databases using SQL DML and DDL; designing relational databases and communicating designs using techniques such as ERDs and normalisation.

Introduction to Business Systems (30 credits)

Brief Summary: The unit introduces the role of information systems in organisations, giving students the opportunity to analyse organisational requirements and develop suitable information system solutions.

Indicative Content: Organisational design and the role information systems play in managing common organisational issues. The principles of information systems and the need for good systems design. Systems development: identifying the need for a new or enhanced system; analysing the requirements of the system and generating initial designs to match requirements; justifying suitable methodologies to aid in the development and implementation of an information system.

Year 1: Trimester 3

Tailored off-the-job activity such as core masterclasses, enrichment activities, carbon literacy, EDI, PREVENT, careers, etc.

Year 2: Trimester 1

IT Project Management (30 Credits)

Brief Summary: This unit examines the management of technology projects, looking in depth at the various processes which constitute technology development lifecycles. You will learn how the analysis, modelling, specification, design, implementation, testing, and maintenance of systems are commonly shaped into specialised project management methodologies. You will gain experience in managing projects using recognised methodologies, whilst presenting your work to both technical and non-technical audiences.

Indicative Content: In addition to taught content on a selection of contemporary project management methodologies and the techniques of which they comprise, a sizeable portion of the unit will be dedicated to practical project work. Students will be provided with a brief and will be invited to complete their project using their choice of project management methodology and reflecting the theory of the taught sessions. The unit will also dedicate taught session time to providing individual support and formative feedback to students as they work through their chosen project. Upon completion, students will report on how they applied chosen project management theory and methodologies to a scenario, and this will form the basis of their assessment.

Computer Networks and Security (15 credits)

Brief Summary: This unit introduces the core principles underpinning the design of both internal corporate computer networks and the wider internet. You will study the architecture of wired and wireless computer networks, how network traffic is directed from its source to its destination, and how the internet is structured and managed. You will also learn the core principles of computer security including common risks and threats, along with ways to mitigate them.

Indicative Content: The unit will cover physical network topology for both wired and wireless networks, introducing TCP/IP networking, IP addresses, routing, and the Domain Name System.

Students will undertake practical tasks working with sockets and connections, IP addresses and DNS records.

Students will learn of common security properties (e.g., Confidentiality, Integrity, Availability) and risks (e.g., Disclosure, Alteration, Denial). Using case studies of computer security incidents, students will learn common classes of security threat (e.g., Insider Attack, Malware), common classes of security vulnerability (e.g., Injection, Overflow) and common approaches to mitigating them (e.g., Access Control, Encryption, Firewalls).

Year 2: Trimester 2

Security Fundamentals (15 credits)

Brief Summary: Introduction to the core concepts of computer security including cryptography, malware, hacking, security considerations for different environments, basic attacks and mitigations using industry standard tools.

Indicative Content: Students will be introduced to the major domains of cyber security in the OWASP categories of builder, breaker, and defender. Students will be introduced to the major legislation in the UK and the challenges of ethics in cyber security, how computers work and mixes technical, and people focused controls to reduce data breaches. With practical exercises covering offensive and defensive security, from hacking, detecting, and mitigating an attack in progress, to the creation of Bash scripts to introduce automation of basic security tasks.

Penetration Testing and Vulnerability (30 credits)

Brief Summary: This unit will introduce students to the process of a penetration test from designing the test and setting the initial scope to resolving vulnerabilities and developing mitigation strategies.

Indicative Content: Students will be introduced to a penetration testing methodology and asked to take the steps from identifying assets to reporting their findings. They will build their skills in reconnaissance, vulnerability assessment and pivoting within a system. Once they have identified vulnerabilities, they are asked to play the role of a security engineer, prioritising and triaging their findings, ensuring that they are tracked as they are fixed, and verifying that a fix is in place.

Year 2: Trimester 3

Tailored off-the-job activity such as core masterclasses, certifications such as AWS Cloud Practitioner Essentials, Green Software, etc..

Year 3: Trimester 1

Advanced Networks (15 credits)

Brief Summary: This unit explores the theoretical and practical operation of computer networks, exploring different models and protocols of networking, and an exploration of contemporary problems and challenges in modern networking solutions.

Indicative Content: The unit covers the principles of modern network systems and focuses on their key operational and technical aspects. Students will learn network fundamental components and protocols, how to configure and secure these networks, and discover the operating mechanics of modern wireless networks such as the Internet of Things.

Security Governance, Policy and Audit (30 credits)

Brief Summary: This unit covers the critical aspects of cyber security governance including ethics, legislation and policy.

Indicative Content: The unit will first introduce the concept of risk and how this relates to the assessment and management of business risk. The application of risk management, in terms of the provision of IT, will be explored alongside how it fits within the wider IT service management frameworks like ITIL. Information security standards such as ISO/IEC 27001 will be reviewed alongside approaches to the implementation and auditing of internal security controls as part of a wider IT policy. The analysis of data, production of appropriate MI, and effective stakeholder communication will also be discussed. The main theory will be delivered through formal lectures alongside supporting seminars and labs to put into practice the theory within a more informal setting.

Year 3: Trimester 2

Incidence Response (15 credits)

Brief Summary: This unit focuses on monitoring servers and responding to attacks and data breaches. The unit introduces students to practical techniques for detecting network-based intrusions using industry-standard tools.

Indicative Content: The unit will take students through the various stages of detecting an incident in order to secure a networked computer system. We will analyse and evaluate security threats and vulnerabilities, perform security risk assessments for a range of information systems and propose solutions. Industry standard software will be used for network traffic monitoring and filtering. We will perform several network attacks in the virtualized environments and use capture techniques to study the behaviour of these attacks and prepare response against these incidents.

Applied Cryptography and Information Security (30 credits)

Brief Summary: This unit offers learners the opportunity to develop an understanding of cryptography and how it is applied within an information security perspective.

Indicative Content: Overview of Security - the need for security; security principles (confidentiality, integrity, availability, access control, authentication and non-repudiation); threats; security mechanisms and security services. Cryptography - symmetric and asymmetric encryption; block and

stream ciphers; encryption algorithms: DES, RSA, AES, etc.; attacks on conventional and public key cryptography; Integrity (hash functions and message authentication codes). Access Control - goals of protocols (authentication and authorisation; key distribution and confirmation); zero knowledge proofs; Fiat-Shamir protocol; PKI; Digital certificates; mediated authentication (Needham-Schroeder protocol); Otway-Rees protocol; Access control lists and capabilities; Multilevel Security; Multilateral Security; Covert channels; Kerberos. Internet Security Protocols and Firewalls - Secure application protocols (SSL/TLS, IPSec: IKE); Components of a firewall, functions, and configurations; Intrusion detection (signature-based IDS, anomaly-based IDS).

Year 3: Trimester 3

Tailored off-the-job activity such as personal development and preparation for final year.

Year 4

Emerging Issues in Security, Privacy and Forensics (30 credits)

Brief Summary: A broad research-based unit, focusing on the technical and societal issues posed by emerging technologies from a security, privacy, and forensics perspective.

Indicative Content: In this unit, various emerging and enabling technology that is contemporary to cyber security and digital forensics will be explored, by employing research. The topics such as application of AI and machine learning to security practices and digital forensics will be reviewed. This unit will introduce topics such as fundamentals of machine learning and AI, supervised and unsupervised learning and application of them on threat/intrusion detection, categorisation, etc, by utilizing various security use cases. We will also explore Internet of Things (IoT) and prevalent security issues and approaches to mitigate security risks on a hyper connected world.

CS Synoptic Project

Brief Summary: Apprentices will complete a work-based project, appropriate to their role and pathway, that has a significant, specified and quantifiable expected benefit for their employer organisation. This can be, for example, based on a specific problem, recurring issue, or a new idea or opportunity, leading to a new or improved product and/or process.

Indicative Content: Apprentices will scope a project in consultation with both their supervisor, employer and independent assessor that enables them to demonstrate the knowledge, skills and behaviours (KSBs) mapped to their pathway for this unit from the degree apprenticeship standard for the Digital and Technology Solutions Professional (DTSP) Integrated Degree.

The apprentice will then plan, undertake and manage the project process through to its completion and the deliverable of a new product and/or process (which may be recommendations for changes to an existing process where appropriate). They may work as part of a team to complete a project, which could include external or internal support, but the project output must be their own work and reflective of their own role and contribution to this wider teamwork.

Apprentices will be expected to evaluate the significance and benefit of their project to their employer organisation, and hence demonstrate critical awareness of the role of their own work in

achieving these benefits. They will therefore record how their achievement of KSBs is demonstrated in their project with a skills mapping to be included in the appendix of the written report.

Reflective Practice for Digital and Technology Solutions Professionals

Brief Summary: Within this unit, learners will reflect on their skills, knowledge and behaviour and identify a gap to address. A portfolio will provide a record of the specific skills and knowledge apprentices have developed and used throughout their degree and provide an opportunity to reflect on their professional development objectives within a report. Learner will complete a training activity to address a gap in their skills and/or knowledge.

Indicative Content: A portfolio will be developed over all 4 years of the degree but only contributions relating to level 6 will be formally assessed within this report. Personal Tutors (PTs) and work mentors will guide apprentices in the development of the portfolio. PTs will review the portfolio from the point of view of its assessment at level 6 and provide formative feedback at set times throughout the degree to guide the apprentice. They will offer advice about developing a well-documented account of the apprentice's development of skills and knowledge and appropriate reflections on their learning and its professional impact. Mentors at work will guide the students from the point of view of documenting their work experience and completion of Personal Development Review objectives.