2016 Suite

OCR
Oxford Cambridge and RSA

Cambridge **TECHNICALS LEVEL 3**

IT

Unit 3

Cyber security

Cambridge TECHNICALS 2016

Y/507/5001

Guided learning hours: 60

Version 3 - revised September 2016

ocr.org.uk/it

LEVEL 3

UNIT 3: Cyber security

Y/507/5001

Guided learning hours: 60

Essential resources required for this unit: none

This unit is externally assessed by an OCR set and marked examination.

UNIT AIM

The need for secure digital systems is more crucial than ever before. We rely on computerised systems and networks to collect, process, store and transfer vast amounts of data and to control critical systems such as water and power supplies. Business and e-commerce can be undertaken twenty four hours a day, seven days a week and telecommunications enable us to keep in touch with family and friends and collaborate with colleagues at any time. Mobile devices offer us freedom and flexibility of where and how we learn and work. However, for all the advantages that these systems offer us, some people have found ways to exploit them and this poses a threat to our safety and security in the real world, as much as in the cyber world. To deal with this problem the cyber security industry is expanding at a rapid rate.

This unit has been designed to enable you to gain knowledge and understanding of the range of threats, vulnerabilities and risks that impact on both individuals and organisations. You will learn about the solutions that can be used to prevent or deal with cyber security incidents resulting from these challenges. You will be able to apply your knowledge and understanding of cyber security issues and solutions by reviewing and making recommendations for ways to best protect digital systems and information.

Learning within this unit will also support the delivery of the Cisco Cyber Security and CompTIA A+, CompTIA Security+, CompTIA Mobility+ qualifications. The unit also makes reference to UK government cyber security initiatives, for example, the UK government's The UK Cyber Security Strategy, Cyber Essentials Scheme, 10 Steps Strategy, and Cyber Streetwise.

TEACHING CONTENT

The teaching content in every unit states what has to be taught to ensure that learners are able to access the highest grades.
Anything which follows an i.e. details what must be taught as part of that area of content. Anything which follows an e.g. is illustrative.

For externally assessed units, where the content contains i.e. and e.g. under specific areas of content, the following rules will be adhered to when we set questions for an exam:

- a direct question may be asked about unit content which follows an i.e.
- where unit content is shown as an e.g. a direct question will not be asked about that example.

Learners are expected to keep up-to-date with the latest developments, innovations and new approaches in cyber security when acquiring knowledge and understanding of this unit content.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
1. Understand what is meant by cyber security	1.1 Cyber security aims to protect information, i.e.: • confidentiality • integrity • availability 1.2 Types of cyber security incidents, i.e.: • unauthorised access including hacking, escalation of privileges • information disclosure including personal information, government information • modification of data • inaccessible data including account lockout, denial of service • destruction including using malware, deliberate erasure • theft including identity, finance, military secrets	Learners should know what is meant by the term cyber security. They should know about digital systems and understand why the information stored on them needs to be kept secure at all times. Leaners should know about the types and nature of cyber security incidents that affect individuals, states and organisations.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	1.3 The importance of cyber security, i.e.: • the need to protect personal data (e.g. health, financial, national insurance) • the need to protect an organisation's data (e.g. financial, research, development plans) • the need to protect a state's data (e.g. economic data, national security)	
2. Understand the issues surrounding cyber security	2.1 Threats to cyber security, i.e. • vulnerabilities o system attacks o physical threats o environmental • accidental • intentional • organised crime • state sponsored 2.2 Types of attackers, i.e.: • hacktivist • cyber-criminal • insider • script kiddie • vulnerability broker • scammers • phishers • cyber-terrorists • characteristics including age, location, social group 2.3 Motivation for attackers, i.e.: • espionage • righting perceived wrongs	Learners should know about the wide range of threats to cyber security including those threats that are accidental or intentional. Learners should know about the types of attacker, their characteristics and their motivations.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	• publicity • fraud • score settling • public good • thrill • income generation 2.4 Targets for cyber security threats, i.e.: • people • organisations • equipment • information • methods that can be used during an attack 2.5 Impacts of cyber security incidents, i.e.: • global problem, individuals, organisations and states • loss including confidentiality, integrity, availability, data, finance, business, identity, reputation, customer confidence • disruption including people's lives, business, industry, transport, industry, the media, utilities • safety including identity theft, oil installations, traffic control 2.6 Other considerations of cyber security, i.e.: • ethical • legal • operational • implications for stakeholders	Learner should know about the different targets for cyber security threats and how these threats might manifest themselves. This should lead to an understanding of the possible impacts from cyber security incidents and how these affect different stakeholders in a variety of different ways. Learners should know about other cyber security considerations. This should lead to an understanding of the implications for different stakeholders in this wider context. Learners should be aware of the latest or most up-to-

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
		date versions of legislation
3. Understand measures used to protect against cyber security incidents	3.1 Cyber security risk management, i.e.: • identify assets and analyse risks • mitigate risks by: o testing for potential vulnerabilities • monitoring and controlling systems • protect vulnerabilities • cost/benefit 3.2 Testing and monitoring measures, i.e.: • vulnerability testing including penetration testing, fuzzing, security functionality, sandboxing • intrusion detection systems (IDS) including network intrusion detection systems (NIDS), host intrusion detection systems (HIDS), distributed intrusion detection system (DIDS), anomaly-based, signature-based, honeypots • intrusion prevention systems (IPS) • emerging technologies • effectiveness 3.3 Cyber security controls (access controls), i.e.: • physical including biometric access, swipe cards, alarms • hardware including cable locks, safes • software including firewalls, anti-malware, operating system updates, patch management • data including in use, at rest, in-transit, in the cloud • encryption including disks, databases, files, removable media, mobile devices • cryptography	Learners should know about the various measures that should be taken to manage cyber security. This should lead to an understanding of, and justification for, different measures that can be taken in a given context. Learners should know about different testing and monitoring measures that can be used to test for vulnerabilities. This should lead to an understanding and justification of the effectiveness of different measures in a given context. Learners should know about the different security controls and their characteristics. This should lead to an understanding and justification of the effectiveness of different controls in a given context.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	• devices including. hard drives, external drives, USBs • procedures including access management, data backup, remote working, device management, user accounts and permissions, awareness and training • emerging technologies • characteristics	
4. Understand how to manage cyber security incidents.	4.1 Responding to an incident, i.e.: • know responsibilities • know who to contact • know procedures • know the extent of the incident • contain the incident • eradicate the incident • reduce the impact of the incident • recover from the incident • confirm the system is functioning normally 4.2 Cyber security incident report, i.e.: • incident title and date of incident • target of the incident • incident category, i.e.: o critical o significant o minor o negligible • description of the incident • type of attacker(s) • purpose of incident • techniques used by the attacker(s) • capability of attacker(s)	Learners should know about different procedures that should be followed in the event of a cyber security incident. This may include conducting investigations or being subject to an investigation. This should lead into an understanding and justification of why certain procedures should be taken in a given context. Learners should know the various stages of investigation that should be undertaken should a cyber security incident occur. This should lead to an understanding of, and justification for decisions that must be taken in a given context. It is possible learners will be asked to complete sections of a cyber security report as part of the examination for this unit.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification

	• impact of the incident on business, data, recovery time
	• cost of the incident
	• responses needed
	• future management
	  o review (of incident)
	  o evaluation to include identification of trends
	  o update of documentation, key information, procedures and controls
	  o recommendations of changes	

LEARNING OUTCOME (LO) WEIGHTINGS

Each learning outcome in this unit has been given a percentage weighting. This reflects the size and demand of the content you need to cover and its contribution to the overall understanding of this unit. See table below:

LO1	5-15%
LO2	35-45%
LO3	20-30%
LO4	10-20%

ASSESSMENT GUIDANCE

All LOs are assessed through externally set written examination papers, worth a maximum of 60, marks and 1 hour in duration.

Learners should study the meaning of cyber security and gain an understanding of its overall purpose. They should study the wide variety of issues surrounding cyber security and the measures that are used to protect against cyber security incidents. Breaches in cyber security can cause serious issues to individuals and organisations and, therefore, learners should have a good understanding of how to manage cyber security incidents.

Exam papers for this unit will include a pre-released case study. The paper will include questions associated with the pre-released case study as well as questions to demonstrate a more general understanding of the subject. Questions will provide sufficient information to support the application and interpretation of the taught content of the unit. During the external assessment, learners will be expected to demonstrate their understanding through questions that require the skills of analysis and evaluation in particular contexts.

Some providers for the industry qualifications offer quizzes, tests and assessments. Reference to these websites may support knowledge and learning.
www.**comptia**.org
www.**cisco**.com/UK

EMPLOYABILITY SKILLS

Employability skills	Learning outcome
Communication	LO4
Critical thinking	LO1, LO2, LO3, LO4
Decision making	LO1, LO2, LO3, LO4

MEANINGFUL EMPLOYER INVOLVEMENT - a requirement for the Diploma (Tech Level) qualifications

The 'Diploma' qualifications have been designed to be recognised as Tech Levels in performance tables in England. It is a requirement of these qualifications for centres to secure for every learner employer involvement through delivery and/or assessment of these qualifications.

The minimum amount of employer involvement must relate to at least one or more of the elements of the mandatory content. This unit is a mandatory unit in all specialist pathways in the Level 3 Cambridge Technical Diploma in IT (720 GLH) and the Level 3 Cambridge Technical Extended Diploma in IT (1080 GLH).

Eligible activities and suggestions/ideas that may help you in securing meaningful employer involvement for this unit are given in the table below.

Please refer to the *Qualification Handbook* for further information including a list of activities that are not considered to meet this requirement.

Meaningful employer involvement	Suggestion/ideas for centres when delivering this unit
1. Learners undertake structured work-experience or work-placements that develop skills and knowledge relevant to the qualification.	As part of a learners work experience they could find out what procedures the business has in place to manage cyber security incidents and how the business protects itself against cyber security incidents (LO3/LO4)
3. Learners take one or more units delivered or co-delivered by an industry practitioner(s). This could take the form of master classes or guest lectures.	An Industry Practitioner could be used to present a guest lecture on how they manage cyber security in their company (LO3).

To find out more
ocr.org.uk/it
or call our Customer Contact Centre on **02476 851509**

Alternatively, you can email us on **vocational.qualifications@ocr.org.uk**

OCR
Oxford Cambridge and RSA