

Cambridge TECHNICALS LEVEL 3

IT

Unit 3 – Cyber security DELIVERY GUIDE

Version 2

Cambridge
TECHNICALS
2016

3.1415926535 8979323846 2643383279
5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095

Phasellus pulvinar varius odio ac placerat. Aliquam mollis justo et tellus blandit ac, aliquet nibh dapibus. Nunc lorem laevis, cursus at aliquam ut, hendrerit aliquam turpis. Pellentesque nec velit quis dui commodo varius ac sed risus. Suspendisse portam. Duis volutpat dapibus pulvinar.

Nunc venenatis, odio quis dicitur eleifend. Curabitur convallis sapien, nec commodo velit dui eget tellus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam non sapien purus. In posuere dolor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

Vivamus sed nibh arcu, id ultricies nulla. Quisque porttitor, quam ut thei dunt gravida, risus laevis rutrum erat, sit amet placerat purus justo nec massa. Class

CONTENTS

Introduction	3
Key Terms	4
Misconceptions	8
Suggested Activities:	
Learning Outcome (LO1) Understand what is meant by cyber security	9
Learning Outcome (LO2) Understand the issues surrounding cyber security	12
Learning Outcome (LO3) Understand measures used to protect against cyber security incidents	19
Learning Outcome (LO4) Understand how to manage cyber security incidents	27
Related Activities	31

The activities within this teaching and learning resource must not be used for summative assessment purposes. As part of our teaching we expect support to be given to your learners; such support is not permissible for summative assessment and is likely to be considered malpractice.

INTRODUCTION

This Delivery Guide has been developed to provide practitioners with a variety of creative and practical ideas to support the delivery of this qualification. The Guide is a collection of lesson ideas with associated activities, which you may find helpful as you plan your lessons.

OCR has collaborated with current practitioners to ensure that the ideas put forward in this Delivery Guide are practical, realistic and dynamic. The Guide is structured by learning outcome so you can see how each activity helps you cover the requirements of this unit.

We appreciate that practitioners are knowledgeable in relation to what works for them and their learners. Therefore, the resources we have produced should not restrict or impact on practitioners' creativity to deliver excellent learning opportunities.

Whether you are an experienced practitioner or new to the sector, we hope you find something in this guide which will help you to deliver excellent learning opportunities.

If you have any feedback on this Delivery Guide or suggestions for other resources you would like OCR to develop, please email resources.feedback@ocr.org.uk.

OPPORTUNITIES FOR ENGLISH AND MATHS SKILLS DEVELOPMENT

We believe that being able to make good progress in English and maths is essential to learners in both of these contexts and on a range of learning programmes. To help you enable your learners to progress in these subjects, we have signposted opportunities for English and maths skills practice within this resource. These suggestions are for guidance only. They are not designed to replace your own subject knowledge and expertise in deciding what is most appropriate for your learners.



English



Maths



Work

Please note

The timings for the suggested activities in this Delivery Guide **DO NOT** relate to the Guided Learning Hours (GLHs) for each unit.

Assessment guidance can be found within the Unit document available from www.ocr.org.uk.

The latest version of this Delivery Guide can be downloaded from the OCR website.

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.

Unit 1 TITLE

LO1	Understand what is meant by cyber security
LO2	Understand the issues surrounding cyber security
LO3	Understand the measures used to protect against cyber security incidents
LO4	Understand how to manage cyber security incidents

To find out more about this qualification please go to: <http://www.ocr.org.uk/qualifications/cambridge-technicals-it-level-3-certificate-extended-certificate-introductory-diploma-foundation-diploma-diploma-05838-05842-2016-suite/>

Cambridge
TECHNICALS
2016

2016 Suite

- New suite for first teaching September 2016
- Externally assessed content
- Eligible for Key Stage 5 performance points from 2018
- Designed to meet the DfE technical guidance

KEY TERMS

Explanations of the key terms used within this unit, in the context of this unit

Key term	Explanation
Access management	Managing the access to a computer system/network. It includes procedures such as account administration, account maintenance, account monitoring and the revocation of an account.
Account lockout	A software security method performed by operating system software that locks any account when a user fails a login attempt more than a set number of times. For example, system software can be set up to lock an account for several hours if the user fails the login three consecutive times in a set time frame.
Anti-malware	Software designed to prevent, detect and eradicate malicious software, such as a virus or a worm.
Anomaly based	Software that is designed to detect computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
Asset	Something that is of value to a person, an organisation or a state, e.g. data, finance and secrets that should be secured against cyber security incidents.
Attacker	Individuals or organisations that target computer systems/networks illegally.
Audit trail	A record of activities on a computer system/network, for example, a record of modifications to data or access to parts of a system/network.
Availability	Data/information stored on a computer system/network must be available to authorised users and organisations and be protected from unauthorised deletion.
Biometric access	Access to a computer system/network using technologies that measure and analyse human body characteristics for authentication purposes, such as DNA, fingerprints, retinas, voice patterns, facial patterns and hand measurements.
Botnet	A network of computers infected with malicious software and controlled without the owners' knowledge, for example, to send spam or hoax emails.
Business continuity plan	A plan to continue operations that an organisation will follow if it is affected by a cyber security incident
Confidentiality	Information stored on a computer system/network must be protected against unintended or unauthorised access. Data confidentiality is a measure of the ability of a system to protect its data.
Cyber criminal	An individual who commits illegal activities using computers and the Internet.
Cyber dependant	Illegal activities dependent on the use of computers and the Internet, such as hacking or the distribution of malware on a network.
Cyber enabled	Illegal activities that could be undertaken without the use of computers, such as fraud but that are enabled by the use of computers, such as fraudulently obtaining money for goods online.

Explanations of the key terms used within this unit, in the context of this unit

Key term	Explanation
Cyber security	Refers to technologies, processes and practices designed to protect computers, networks, software and data from attack, damage or unauthorised access and aims to protect data confidentiality, integrity and availability.
Cyber security incident	An unwanted/unexpected event, such as an intrusion into a computer system/network, such as the spread of malware.
Cyber security incident report	A report that documents the details of a cyber security incident, such as the type of incident, when it occurred, how it was performed, etc.
Denial of service	An attempt to disrupt a network/business/organisation by issuing more requests than a system is able to cope with, it can be performed with malicious intent or as a protest.
Disaster recovery plan	A plan that documents a set of procedures for an organisation to follow in order to recover and protect a computer system and its data in the event of a cyber security incident.
Encryption	A method that is used to attempt to ensure data security by use of encrypted (secret) code. In order to read the contents of an encrypted message or file, someone must have access to a secret key or password that will enable them to decrypt the message or file.
Escalation of privileges	Exploiting a weakness or weaknesses in an operating system or software application, such as a bug, design flaw or configuration oversight and gaining elevated access to resources that are normally protected.
Ethical hacking	An individual who attempts to penetrate a computer system/network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. He or she is also known as a white hat hacker. He or she can also work alone.
Firewall	Software that is designed to protect a computer system/network from unauthorised access and intrusion.
Fuzzing	A method that is used to test the security of software.
Hacking	A method of gaining unauthorised access to a computer system/network.
Hacker	An individual who gains unauthorised access to a computer system/network.
Hacktivist	An individual who gains unauthorised access to computer system/network for social or political purposes.
Hoax email	Usually an email message warning recipients of a non-existent threat, usually forging quotes supposedly from authorities such as Microsoft and IBM.

Explanations of the key terms used within this unit, in the context of this unit

Key term	Explanation
Honeypot	Decoy servers or computer systems that are set up to gather information on intruders or attackers of computer systems/networks.
Host firewall	Software that runs on a single host computer that restricts incoming and outgoing network activity for that host computer only. It can be used to prevent a host computer from becoming infected and stop infected host computers from spreading malware to other hosts computers.
Insider	An individual working inside an organisation, a trusted employee, who performs an illegal action, such as hacking.
Integrity	Integrity of data aims to protect data from unauthorised modification.
Intrusion detection system	Software that monitors network or system activities for unexpected or malicious activities.
Intrusion prevention system	Software that examines network traffic flows to detect and prevent vulnerability exploits.
Malware	Software that is designed to cause disruption or damage to data and/a computer system/network.
Mitigate	To lessen an impact, for example, the impact of a cyber security incident or a risk.
Patch management	Acquiring, testing and installing code changes or patches to software on a computer system/network.
Penetration testing	A software tool that tests a computer system/network to find vulnerabilities that could be exploited by an attacker.
Phisher	An individual that attempts to acquire personal information, often for malicious reasons, such as fraud, by pretending to be a known and trusted individual or organisation.
Phishing	The act of attempting to acquire personal information, often for malicious reasons, such as fraud, by pretending to be a known and trusted individual or organisation.
Non repudiation	Ensures that an individual cannot deny the authenticity of their signature on a document or the sending of a message that they sent.

Explanations of the key terms used within this unit, in the context of this unit

Key term	Explanation
Risk	A threat to a computer system/network can result in a risk, for example, if a hacker gains access to a person's computer, there is a risk that data will be stolen.
Risk analysis	This involves analysing a computer system or a set of procedures and assessing whether a system is at risk from a cyber incident due to weaknesses or vulnerabilities in software, hardware or procedures.
Risk management	This refers to ensuring that risks are monitored carefully and mitigated against or eliminated from a computer system/network.
Sandboxing	This is a security method for separating running programs on a computer system/network. It is often used to run untested code, or untrusted programs from unknown sources such as suppliers, untrusted users and untrusted websites.
Scammer	An individual who attempts to gain, for example, money from another person by fraudulent means enabled by the use of computers and the Internet.
Script kiddie	An individual who uses existing computer scripts or codes to hack into computer systems. They do not have the expertise to write their own code.
Signature based	A digital signature is code that is attached to an electronically transmitted document to verify its contents and the sender's identity.
Social engineering	Hackers use this non-technical method to access computer systems/networks without authorisation. It involves fooling people into breaking normal security procedures, such as guarding their passwords and relies on manipulating the good nature of individuals.
Spyware	Malware software that is designed to obtain covert information about someone else's computer activities by transmitting data covertly, from their hard drive, for example key logging software.
Threat	An action that when performed on a computer system/network can cause destruction or disruption, for example, a hack or malware.
Unauthorised access	Gaining access into a computer system/network illegally.
Virus	Malicious software which is capable of copying itself and corrupting computer systems/networks or destroying data.
Vulnerability	Is a weakness in a computer system/network that can be exploited by a threat, for example, out of date anti-malware software can result in the threat of a malware attack. If a computer system/network's vulnerabilities can be found and dealt with, this will help to minimize threats and risks.
Vulnerability broker	An individual who exploits a vulnerability or weakness in a computer system/network for gain, for example, a hacker.

MISCONCEPTIONS



Some common misconceptions and guidance on how they could be overcome


What is the misconception?	How can this be overcome?	Resources which could help
<p>The difference between vulnerability, threat and risk</p>	<p>Learners often confuse the terms vulnerability, threat and risk. Explanations and examples, such as those referred to in the resources link, may be a way for learners to understand and remember the difference.</p>	<p>Assessment Types - CompTIA Security+ SY0-401: 3.7</p> <p>CompTIA</p> <p>https://www.youtube.com/watch?v=KXuKfckeHzs</p> <p>A video that discusses the differences between risks, vulnerabilities and threats.</p>
<p>The difference between a virus, a worm, a Trojan and a bot</p>	<p>Learners sometimes do not understand the differences between a virus, a worm, a Trojan and a bot. Explanations and examples, such as those referred to in the three resources links, may be a way for learners to understand and remember the differences between the terms.</p>	<p>What Is the Difference: Viruses, Worms, Trojans, and Bots?</p> <p>Cisco</p> <p>http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html</p> <p>A webpage that discusses the differences between viruses, worms, Trojans, and Bots?</p> <p>Malware Overview - CompTIA Security+ SY0-401: 3.1</p> <p>CompTIA</p> <p>https://www.youtube.com/watch?v=fpX5mym4Lfg</p> <p>A short video that discusses types of malware.</p> <p>Botnets - CompTIA Security+ SY0-401: 3.1</p> <p>CompTIA</p> <p>https://www.youtube.com/watch?v=Z8KtojO5eGI</p> <p>A short video that discusses what Botnets are and how they work.</p>

SUGGESTED ACTIVITIES



LO No:	1		
LO Title:	Understand what is meant by cyber security		
Title of suggested activity	Suggested activities	Suggested timings	Also related to
Confidentiality, integrity and availability of digital systems	<p>Tutors could begin by introducing learners to the terms <i>confidentiality, integrity and availability</i> in the context of cyber security and check that they understand what is meant by each term in this context.</p> <p>The following web page provides a broad definition of cyber security that makes reference to confidentiality, integrity and availability</p> <p>http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx</p> <p>Learners could be tasked to research several examples of cyber security incidents and document the following:</p> <p>Incidents where confidentiality has been compromised</p> <p>Incidents in which integrity has been compromised</p> <p>Incidents in which availability has been compromised</p> <p>Incidents in which a combination of confidentiality, integrity and availability have been compromised.</p> <p>Learners could refer to the following resources:</p> <p>NHS has repeated data breaches http://www.bbc.co.uk/news/health-30037938</p> <p>UK sales teams are the most exposed to cyber attacks, study reveals http://www.computerweekly.com/news/4500249735/UK-sales-teams-are-the-most-exposed-to-cyber-attacks-study-reveals</p> <p>Top US Official Quits After Massive Government Hack http://www.securityweek.com/top-us-official-quits-after-massive-government-hack-0</p> <p>Catching the Big Phish: What Are the Security Risks Facing Financial Organisations? http://www.huffingtonpost.co.uk/david-emm/security-risks-facing-financial-organisations_b_7601596.html</p>	1 – 2 hours	Unit 3 LO2, LO3 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2





Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Confidentiality, integrity and availability of digital systems</p> 	<p>Ryanair remains tight-lipped over £3.3m hacker theft http://www.computerweekly.com/news/4500245366/Ryanair-remains-tight-lipped-over-33m-hacker-theft</p> <p>Internet of things: businesses must overcome data and privacy hurdles http://www.theguardian.com/media-network/2015/jun/01/internet-of-things-businesses-data-privacy</p> <p>Smart TVs pose major security risk to government, healthcare and energy companies http://www.ibtimes.co.uk/samsung-smart-tvs-pose-major-security-risk-government-healthcare-energy-companies-1504223</p> <p>Learners also could be tasked to document instances of when the confidentiality, integrity and availability of their data and/or the data of someone that they know, has been compromised.</p> <p>Learners could present their findings and/or personal experiences in the form of a report.</p>	<p>1 – 2 hours</p>	<p>Unit 3 LO2, LO3 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2</p>
<p>The importance of keeping data secure</p> 	<p>Tutors could begin by introducing learners to the different types of data that need to be kept secure: personal data, an organisation's data and a state or country's data.</p> <p>Learners could work in pairs or small groups and list as many types of personal data, organisational data and national data as possible.</p> <p>Learners could present their findings to the rest of the class which could then encourage discussion.</p> <p>They could then consider cases in which data has been compromised:</p> <p>https://www.youtube.com/watch?v=0p3787JiFgQ</p> <p>A short video (8 minutes) by VM news, '10 Cyber Security Facts'</p> <p>The following video (42 minutes), 'Secret International Cyber War Dividing Nations' presents an overview of the issue of cyber war and the battle for data held by organisations and countries.</p> <p>https://www.youtube.com/watch?v=zAS-agcQqEk</p>	<p>1 hour</p>	<p>Unit 3 LO2, LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2</p>


Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Types of cyber security incidents</p> <p>See lesson element Types of cyber security incidents</p> 	<p>Tutors could begin by introducing learners to the term <i>cyber security incident</i> and the types of incidents that can occur.</p> <p>Learners could be tasked to research the following types of cyber security incidents and provide details of at least one example of each type of incident that they research.</p> <p>Hacking Disclosure of government information Impairing the operation of a digital system Denial of service Malware Identity theft</p> <p>Learners could refer to the following resources:</p> <p>BBC News: Cyber Security http://www.bbc.co.uk/news/technology-28549494</p> <p>Computer Weekly http://www.computerweekly.com</p> <p>Security Week http://www.securityweek.com/cybercrime</p> <p>The Huffington Post http://www.huffingtonpost.co.uk/news/cybersecurity/</p> <p>The Telegraph http://www.telegraph.co.uk/technology/internet-security/</p> <p>The Guardian http://www.theguardian.com/small-business-network/series/cyber-security</p> <p>International Business Times: Cyber Security http://www.ibtimes.co.uk/cybersecurity</p> <p>All your devices can be hacked, an article that provides an overview of the problems of cyber crime. http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked</p> <p>NATO and cyber security, Information by NATO on the cyber security issues that it faces. http://www.nato.int/cps/en/natolive/topics_78170.htm</p> <p>Learners could present their findings in the form of a presentation.</p>	<p>1 – 2 hours</p>	<p>Unit 3 LO2, LO3 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2</p>



SUGGESTED ACTIVITIES



LO No:	2		
LO Title:	Understand the issues surrounding cyber security		
Title of suggested activity	Suggested activities	Suggested timings	Also related to
Weaknesses that leave a digital system vulnerable to attack 	<p>Tutors could begin by introducing the term <i>vulnerability</i> and check that learners understand its meaning.</p> <p>Learners could be tasked with assessing the software, hardware, network and people vulnerabilities of the systems that they use in school/college/work/home.</p> <p>Learners could refer to the following resource:</p> <p>A video (39 minutes) on Security Concepts: Computer Security Lectures 2014/15 S2, An overview of cyber security issues (Leeds Beckett University)</p> <p>https://www.youtube.com/watch?v=pLEVNI8KtO4&list=PLUhmDd3hilSIAbnD8eWIDjetsj1eJmiZs</p> <p>A video (5 minutes) on Social Engineering - CompTIA Network+ N10-006 - 3.2, A short introduction to the issue of social engineering.</p> <p>https://www.youtube.com/watch?v=xcJV2JGeVn0</p> <p>They could present their findings in the form of a report or an information leaflet.</p>	2 hours	Unit 3 LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2
The types of threats that digital systems face 	<p>Tutors could begin by introducing the term <i>threat</i> and check that learners understand its meaning.</p> <p>Tutors could then introduce the types of threat that digital systems face.</p> <p>Learners could be tasked with reading through the Sophos guide to computer and data security threats.</p> <p>Sophos</p> <p>Threatsaurus The A-Z of computer and data security threats</p> <p>https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en</p>	2 hours	Unit 3 LO1, LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2


Title of suggested activity	Suggested activities	Suggested timings	Also related to
	<p>Learners could be tasked with reading the following GCHQ document:</p> <p>Cert UK Common Cyber Attacks: Reducing the Impact https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf</p> <p>Learners could also be shown the following videos:</p> <p>New Threats and Security Trends - CompTIA Security+ SY0-401: 2.6 A short introduction to threats and emerging cyber security concerns. A video (2 minutes) https://www.youtube.com/watch?v=Tec1Yg7HMMg</p> <p>Introduction to Computer Security - Information Security Lesson #1 of 12 Discusses threats, risks, vulnerabilities, types of attackers, targets and impacts A video (41 minutes) https://www.youtube.com/watch?v=zBFB34YGK1U</p> <p>Learners could then be tasked with creating a quiz of at least ten questions based on the information that they have read and watched/listened to.</p> <p>Learners could then present their quiz and the class could work through the questions.</p>		
<p>Types of attacks to digital systems</p> 	<p>Tutors could begin by introducing the term <i>attack</i> in the context of cyber security and check that learners understand the meaning in this context.</p> <p>Tutors could then introduce the types of cyber attacks that digital systems face.</p> <p>Learners could be tasked to document information on cyber attacks – they could create a ‘top ten’ in order of severity of impact.</p> <p>Learners could refer to the following resources:</p> <p>Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. A detailed overview of the impacts and costs of cybercrime. A pdf document http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf</p> <p>25 Biggest Cyber Attacks In History - Discusses cyber security incidents A video (14 minutes) https://www.youtube.com/watch?v=Zl_BQoJqCIM</p> <p>Learners could present the details of their top ten in the form of a presentation or information leaflet.</p>		

Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Types of malware</p> 	<p>Tutors could begin by introducing the term <i>malware</i> and check that learners understand its meaning.</p> <p>Learners could be tasked to work in pairs or small groups and research the following malware (one example per pair or group):</p> <p>Zero Day. Heartbleed. Stuxnet. SQL Injection.</p> <p>Learners could refer to the following resources:</p> <p>Malicious Code (Malware) - Information Security Lesson #4 of 12 - an introduction to malicious malware. A video (30 minutes) https://www.youtube.com/watch?v=wn-uVP8HncA</p> <p>Zero-day Attacks - CompTIA Network+ N10-006 - 3.2 - an overview of the issue of Zero Day malware. A video (4 minutes) https://www.youtube.com/watch?v=KG8kFakfS7w</p> <p>SQL Injection, XML Injection, and LDAP Injection - CompTIA Security+ SY0-401: 3.5 - an introduction to the issue of malware injections. A video (5 minutes) https://www.youtube.com/watch?v=Tjc6xYjh46g</p> <p>Heartbleed malware - an introduction to the issue of Heartbleed malware. A Web page http://www.interpol.int/Crime-areas/Cybercrime/Advice/Heartbleed-bug</p> <p>An Unprecedented Look at Stuxnet, the World's First Digital Weapon - a discussion of Stuxnet malware. A Web page http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/</p> <p>Learners could present their findings to the rest of the class in the form of a presentation or create an information leaflet.</p>	2 hours	<p>Unit 3 LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2</p>



Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Don't go phishing!</p> <p>See lesson element Don't Go Phishing!</p> 	<p>Tutors could begin by introducing the term <i>phishing</i> and check that learners understand its meaning.</p> <p>Learners could be tasked to work in pairs or small groups and research types of phishing.</p> <p>Learners could refer to the following resources: http://www.net-security.org/secworld.php?id=18153</p> <p>An example of a phishing scam that affected Virgin Media customers in March 2015. It presents a fake PayPal phishing page. http://www.net-security.org/secworld.php?id=18153</p> <p>A video produced by CompTIA. It is a short introduction to man-in-the-middle attacks https://www.youtube.com/watch?v=p4pLVN_hVsU</p> <p>A video produced by CompTIA. It is a short introduction to vishing. https://www.youtube.com/watch?v=aL_m6jelF1M</p> <p>A video produced by CompTIA. It is a short introduction to whaling. https://www.youtube.com/watch?v=lasCylKGwIA</p> <p>This discusses spear phishing in some detail. http://www.cpni.gov.uk/documents/publications/2013/2013053-spear-phishing-understanding-the-threat.pdf?epslanguage=en-gb</p> <p>This discusses how to recognize phishing email messages or links. https://www.microsoft.com/en-gb/security/online-privacy/phishing-symptoms.aspx</p> <p>This web page discusses phishing. http://www.actionfraud.police.uk/fraud-az-phishing</p> <p>This web page discusses spear phishing. https://www.fishnetsecurity.com/6labs/blog/tip-spear-phishing-or-spearphishing</p> <p>This web page discusses whaling. http://www.scambusters.org/whaling.html</p> <p>Learners could then be tasked with presenting their findings to the rest of the class.</p>	2 hours	Unit 3 LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO1


Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>A rogues' gallery</p> 	<p>Tutors could begin by introducing the term <i>attacker</i> in the context of cyber security and check that learners understand its meaning in this context.</p> <p>Learners could be tasked with creating a 'rogues gallery' of digital system attackers.</p> <p>The 'gallery' could include reference to six types of attackers and for each type of attacker, there should be an example included of the type of attack that they are associated with undertaking.</p> <p>Learners could refer to the following resource:</p> <p>Insider Threats - CompTIA Network+ N10-006 - 3.2 - an introduction to the issue of threats posed by 'insiders'.</p> <p>A video (4 minutes) https://www.youtube.com/watch?v=Urc-My8AnBY</p> <p>Introduction to Computer Security - Information Security Lesson #1 of 12 Discusses threats, risks, vulnerabilities, types of attackers, targets and impacts</p> <p>A video (41 minutes) https://www.youtube.com/watch?v=zBFB34YGK1U</p> <p>Police shut down network 'used to steal bank details', February 2015</p> <p>An online new article. http://www.bbc.co.uk/news/technology-31622306</p> <p>Learners could present their work to the class in the form of a presentation.</p>	2 hours	Unit 3 LO1, LO3, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2
<p>Why digital systems are attacked</p> 	<p>Learners could be tasked with creating a game or a quiz in which other learners are asked to match a profile/characteristic to a type of digital system attacker.</p> <p>Learners could refer to the following resource:</p> <p>The secret lives of hackers – A short introduction to hacking – who does it and what are their motivations?</p> <p>A video (3 minutes) www.youtube.com/watch?v=DKzi5CYNFAg</p> <p>Learners could present their game or quiz and the other learners could attempt to match the profile/characteristic to the perpetrator of an attack.</p>	1 – 2 hours	Unit 3 LO1, LO4 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2



Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Is hacking ever ethical?</p> 	<p>Tutors could begin by introducing the term <i>ethical hacking</i> and check that learners understand its meaning.</p> <p>Tutors could then introduce the term <i>hacktivism</i> and check that learners understand its meaning.</p> <p>Learners could be tasked to work in pairs or small groups and document their responses to the question <i>is hacking ever ethical?</i></p> <p>Learners could refer to the following resources:</p> <p>The Law and Ethics</p> <p>http://www.bigambition.co.uk/secure-futures/resources/teachers3/</p> <p>These resources include a session plan, a presentation, questions and answers relating to hacking and the law, ethical dilemmas discussions, different types of hackers and a questions and answers.</p> <p>Learners could present their responses to the class in the form of a presentation.</p>	1 – 2 hours	Unit 3 LO1
<p>Should emails be monitored?</p> 	<p>Tutors could begin by introducing the term <i>surveillance</i> and check that learners understand its meaning.</p> <p>Learners could be tasked to work in pairs/groups and document their responses to the question <i>should emails be monitored?</i></p> <p>Learners could refer to the following resource:</p> <p>Personal Privacy and Security: Computer Security Lectures 2014/15 S2 – An overview of personal privacy and cyber security. (Leeds Beckett University).</p> <p>A video (39 minutes)</p> <p>https://www.youtube.com/watch?v=ffLlhPszqbo&list=PLUhmDd3hiISIAbnD8eWIDjetsj1eJmiZs&index=2</p> <p>A sensible way forward on surveillance? An online article that discusses the issue of surveillance.</p> <p>http://www.bbc.co.uk/news/uk-33092737</p> <p>Learners could present their responses to of the class in the form of a presentation.</p>	1 – 2 hours	Unit 3 LO1


Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Legal requirements</p> 	<p>Tutors could begin by introducing the role of law in cyber security and check that learners understand the part that law plays in cyber security.</p> <p>Learners could be tasked to work through the following resources:</p> <p>The Law and Ethics</p> <p>http://www.bigambition.co.uk/secure-futures/resources/teachers3/</p> <p>These resources include a session plan, a presentation, questions and answers relating to hacking and the law, ethical dilemmas discussions, different types of hackers and a questions and answers.</p>	<p>1 – 2 hours</p>	<p>Unit 3 LO1, LO3 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 17 LO2 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1 Unit 22 LO2</p>


SUGGESTED ACTIVITIES


LO No:	3		
LO Title:	Understand the measures used to protect against cyber security incidents		
Title of suggested activity	Suggested activities	Suggested timings	Also related to
Identifying assets 	<p>Tutors could begin by introducing the term <i>asset</i> in the context of cyber security and check that learners understand its meaning in this context.</p> <p>Learners could be tasked with listing their personal assets.</p> <p>Learners could also be tasked with listing the assets of a local/national business or industry.</p> <p>Learners could present their work in the form of an inventory.</p>	1 hour	Unit 3 LO1, LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2
Identifying risks 	<p>Tutors could begin by introducing the term <i>risk</i> in the context of cyber security and check that learners understand its meaning in this context.</p> <p>Learners could be tasked with assessing the risks if their assets are impacted by a cyber security incident.</p> <p>Learners could also be tasked with assessing the risks if the assets of a local or national business or industry are impacted by a cyber security incident.</p> <p>Learners could refer to the following resource:</p> <p>Cyber Risks An overview of the risks to cyber security.</p> <p>A video (36 minutes) https://www.youtube.com/watch?v=K1BKhpzW8TA</p> <p>Introduction to Risk Assessment – an overview of risk assessment.</p> <p>A video (57 minutes) https://www.youtube.com/watch?v=EWdfovZlg2g</p> <p>Learners could present their work in the form of an information leaflet.</p>	1 hour	Unit 3 LO1, LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2

Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Testing and monitoring digital systems</p> 	<p>Learners could be given the opportunity to work on a machine(s) that offers desktop virtualisation and check that software patches are up to date, create passwords on files, implement access levels linked to usernames and capture evidence of a threat or attempt at illegal access.</p> <p>Learners could also refer to the following resources:</p> <p>Vulnerability Scanning – CompTIA Security+ SY0-401: 3.8 – an introduction to vulnerability testing.</p> <p>A video (8 minutes) https://www.youtube.com/watch?v=kC3Egf53VE</p> <p>Fuzzing – CompTIA Security+ SY0-401: 4.1 – an introduction to the fuzzing technique of testing.</p> <p>A video (4 minutes) https://www.youtube.com/watch?v=CdAekWEN4wA</p> <p>Denial of Service and Intrusion Detection – Information Security Lesson #11 of 12 – an overview of denial of service and intrusion detection.</p> <p>A video (27 minutes) https://www.youtube.com/watch?v=0_59AocrBVo</p> <p>The Honeypot Project – an overview of the use of honeypots.</p> <p>A website http://www.honeynet.org/</p> <p>Cisco Network-Based Intrusion Prevention Case Study on network-based intrusion prevention.</p> <p>Web pages http://www.cisco.com/web/about/ciscoatatwork/security/csirt_network-based_intrusion_prevention_system_web.html</p>	<p>1 – 2 hours</p>	<p>Unit 3 LO1, LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2</p>

Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Physical controls that can be used to secure digital systems</p> 	<p>Learners could be presented with a scenario/case study of a fictitious company OR make reference to a real, well known company and tasked to recommend physical controls that they would expect the company to use to secure their data.</p> <p>Learners could refer to the following resource:</p> <p>Physical Security Controls – CompTIA Network+ N10-006 – 3.4 – an introduction to physical security controls.</p> <p>A video (5 minutes) https://www.youtube.com/watch?v=xat110UGTRU</p> <p>Learners could present their recommendations in the form of an information guide for a small business.</p>	1 hour	Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2
<p>Hardware controls used to secure digital systems</p> 	<p>Learners could be presented with a scenario/case study of a fictitious company.</p> <p>Alternatively or in addition, they could make reference to a digital system that they use and/or a digital system used by a well-known organisation. They could be tasked to recommend hardware controls that they would expect an organisation to use to secure their data. If discussing their own digital system, they could be tasked to suggest what hardware controls they should have in place.</p> <p>Learners could refer to the following resources:</p> <p>Hardware Security – CompTIA Security+ SY0-401: 4.3 – An introduction to hardware security controls.</p> <p>A video (4 minutes) https://www.youtube.com/watch?v=BqvV6SOBVLs</p> <p>Learners could be asked to apply their knowledge of hardware controls to produce a guide recommending the use of hardware controls to staff at an organisation. If they are making reference to their own digital system, they could provide information in the form of a presentation.</p>	1 hour	Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2


Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Software controls used to secure digital systems</p> <p>See lesson element</p> <p><i>Software controls used to secure digital systems</i></p> 	<p>Learners could be presented with a scenario/case study of a fictitious company.</p> <p>Alternatively or in addition, they could make reference to a digital system that they use and/or make reference to a digital system that is used by a well-known organisation.</p> <p>They could be tasked to recommend software controls that they would expect an organisation to use to secure their data. If discussing their own digital system, they could be tasked to suggest what software controls they should have in place.</p> <p>Learners could refer to the following resource:</p> <p>https://www.youtube.com/watch?v=7Kq1bBxUqLM This video presents a short introduction to anti-malware software.</p> <p>https://www.youtube.com/watch?v=XEqnE_sDzSk This video presents an overview of firewalls and network security.</p> <p>https://www.youtube.com/watch?v=pT_aSqHq3hU This video produced by CompTIA, presents a short introduction to operating system security and settings.</p> <p>https://www.youtube.com/watch?v=IDCgSbrKKGc This video produced by CompTIA, presents a short introduction to patch management.</p> <p>https://www.youtube.com/watch?v=wu3CNkaoVml This video produced by CompTIA, presents a short introduction to managing password policies.</p> <p>http://www.cpni.gov.uk/advice/cyber/Patching/ The above web page discusses the importance of patching to prevent against an attack to software.</p> <p>http://www.itgovernance.co.uk/boundary-firewalls-and-internet-gateways.aspx#.VZfRkFLD9sE The above web pages discuss the importance of firewalls.</p> <p>http://www.itgovernance.co.uk/patch-management.aspx#.VzfWa1LD9sE The above web pages discuss software vulnerabilities and a related case study.</p> <p>http://www.itgovernance.co.uk/malware-protection.aspx#.VZfW2VLD9sE The above web pages discuss the importance of malware protection.</p>	1 – 2 hours	Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2

Title of suggested activity	Suggested activities	Suggested timings	Also related to
	<p>http://www.microsoft.com/security/portal/threat/threats.aspx The above web pages produced by Microsoft discuss the importance of malware protection.</p> <p>http://www.sans.org/critical-security-controls/control/5 The above web pages discuss the importance of malware.</p> <p>http://www.sans.org/critical-security-controls/control/6 The above web pages discuss the importance of securing application software.</p> <p>Learners could present their recommendations in the form of a presentation.</p>		
<p>Data controls used to secure digital systems</p> 	<p>Learners could be presented with a scenario/case study of a fictitious company OR make reference to a real, well known company and tasked to recommend data controls that they would expect the company to use to secure their data.</p> <p>Learners could refer to the following resource:</p> <p>States of Data – CompTIA Security+ SY0-401: 4.4 – an introduction to securing data in-transit, at-rest, and in-use.</p> <p>A video (5 minutes) https://www.youtube.com/watch?v=OfWZmxrvUgl</p> <p>Learners could present their recommendations in the form of an information guide for a small business moving into e-commerce.</p>	1 hour	Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2



Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Encryption controls used to secure digital systems</p> 	<p>Tutors could begin by introducing the term <i>encryption</i> and check that learners understand its meaning.</p> <p>Learners could work in pairs or small groups and each pair or group tasked with researching two commonly used methods of encryption.</p> <p>Learners could refer to the following resources:</p> <p>Encryption Concepts – Information Security Lesson #6 of 12 – an overview of encryption techniques.</p> <p>A video (1 hour) https://www.youtube.com/watch?v=qcai6ZY6sVs</p> <p>Encryption Part I: Introduction to Encryption 1 – an overview of asymmetric encryption and hashing.</p> <p>A video (12 minutes) https://www.youtube.com/watch?v=KEWGoXE6zMo</p> <p>Data Encryption – CompTIA Security+ SY0-401: 4.4 - an introduction to data encryption.</p> <p>A video (8 minutes) https://www.youtube.com/watch?v=7Cfinirgcl4</p> <p>Hardware-based Encryption – CompTIA Security+ SY0-401: 4.4 – an introduction to hardware based encryption.</p> <p>A video (6 minutes) https://www.youtube.com/watch?v=eWCCYXywfOI</p> <p>Cryptography Overview – CompTIA Security+ SY0-401: 6.1 – an introduction to cryptography.</p> <p>A video (8 minutes) https://www.youtube.com/watch?v=W5su65wwd0g</p> <p>Non-Repudiation – CompTIA Security+ SY0-401: 6.1 – an introduction to non-repudiation and digital signatures.</p>	<p>1 – 2 hours</p>	<p>Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2</p>

Title of suggested activity	Suggested activities	Suggested timings	Also related to
	<p>A video (5 minutes) https://www.youtube.com/watch?v=4w2MTKx4d6A</p> <p>Steganography – CompTIA Security+ SY0-401: 6.1 - an introduction to steganography.</p> <p>A video (4 minutes) https://www.youtube.com/watch?v=WIYdHRNeHEA</p> <p>Strong vs. Weak Encryption – CompTIA Security+ SY0-401: 6.2 – an introduction to strong and weak encryption techniques.</p> <p>A video (3 minutes) https://www.youtube.com/watch?v=h7QwYjZ0sz0</p> <p>Learners could present their findings in the form of a report or a presentation.</p>		
<p>Controls that are required for personal devices</p>	<p>Learners could be tasked to produce an information leaflet for learners and staff that makes them aware of the device controls that they should follow when bringing their own devices to school/ college.</p> <p>Alternatively or in addition, learners could be tasked to produce an information leaflet for staff at a workplace that makes them aware of the device controls that they should follow when bringing their own devices to work.</p> <p>Learners could refer to the following resources:</p> <p>Mobile BYOD Concerns – CompTIA Security+ SY0-401: 4.2 – an introduction to the issues of security and bringing devices to work.</p> <p>A video (8 minutes) https://www.youtube.com/watch?v=hiHLGSTCDf8</p> <p>Mobile Application Security – CompTIA Security+ SY0-401: 4.2 – an introduction to mobile application security.</p> <p>A video (6 minutes) http://how-tofind.com/tube/2D6vtgwZvn0/mobile-device-security-comptia-security-sy0-301-4-2</p> <p>Mobile Device Security – CompTIA Security+ SY0-401: 4.2 – an introduction to mobile device security.</p> <p>A video (4 minutes) https://www.youtube.com/watch?v=4j4hRCnMjEw</p> <p>Learners could present their findings in the form of a report, an information guide or a presentation.</p>	1 – 2 hours	<p>Unit 3 LO2, LO4</p> <p>Unit 1 LO5</p> <p>Unit 2 LO4, LO6</p> <p>Unit 4 LO1, LO2, LO3</p> <p>Unit 7 LO2</p> <p>Unit 11 LO2</p> <p>Unit 12 LO1</p> <p>Unit 18 LO2</p> <p>Unit 19 LO1, LO2</p> <p>Unit 20 LO2</p> <p>Unit 21 LO1, LO2</p> <p>Unit 22 LO2</p>




Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>Procedures to keep data secure</p> 	<p>Learners could be tasked to produce a set of procedures that everyone at home needs to follow when using a digital system.</p> <p>Alternatively or in addition, learners could be tasked to produce a set of procedures that staff and learners at school/college need to follow or staff in a workplace when using digital systems.</p> <p>Learners could refer to the following resources:</p> <p>Data Policies – CompTIA Security+ SY0-401: 4.4 – an introduction to policies to secure data. A video (5 minutes) https://www.youtube.com/watch?v=K6VudXYafZw</p> <p>Managing Password Policies – CompTIA Security+ SY0-401: 5.3 - an introduction to managing password policies. A video (4 minutes) https://www.youtube.com/watch?v=wu3CNkaoVml</p> <p>Privileges – CompTIA Security+ SY0-401: 5.3 – an introduction to user privileges. A video (4 minutes) https://www.youtube.com/watch?v=NXOQMGYuwoo</p> <p>User Access Reviews and Monitoring – CompTIA Security+ SY0-401: 5.3 - an introduction to user access reviews and monitoring. A video (4 minutes) https://www.youtube.com/watch?v=HvMJRFYn7Ik</p> <p>Access control and administrative privilege management – an overview of risks associated with access control and administrative privilege management and a related case study. Web pages http://www.itgovernance.co.uk/access-control-and-administrative-privilege.aspx#.VZfUBFLD9sE</p> <p>Bring your own devices (BYOD) – an overview of BYOD issues. PDF document https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.Pdf</p> <p>Account monitoring and control – an overview of account monitoring and control. Web pages http://www.sans.org/critical-security-controls/control/16</p> <p>Learners could present their work in the form of an information guide to an organisation.</p>	1 – 2 hours	Unit 3 LO2, LO4 Unit 1 LO5 Unit 2 LO4, LO6 Unit 4 LO1, LO2, LO3 Unit 7 LO2 Unit 11 LO2 Unit 12 LO1 Unit 18 LO2 Unit 19 LO1, LO2 Unit 20 LO2 Unit 21 LO1, LO2 Unit 22 LO2


SUGGESTED ACTIVITIES

LO No:	4		
LO Title:	Understand how to manage cyber security incidents		
Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>How to respond to a cyber security incident at home</p> 	<p>Tutors could begin by introducing learners to the different procedures that should be followed in the event of a cyber security incident.</p> <p>Learners could be tasked to document how they would respond to a cyber security incident that happened at home.</p> <p>Learners could refer to the following resource:</p> <p>Live System Analysis – part 2: Computer Security Lectures 2014/15 S1 – discusses how to respond to a cyber security incident</p> <p>A video (25 minutes) https://www.youtube.com/watch?v=7MhCz6Kl1To</p> <p>Learners could present their work in the form of a report, an information leaflet or a presentation.</p>	1 hour	Unit 3 LO3
<p>How to respond to a cyber security incident at school/ college</p> 	<p>Tutors could begin by introducing learners to the different procedures that should be followed in the event of a cyber security incident.</p> <p>Learners could be tasked to document how they would respond to a cyber security incident that happened at school/college.</p> <p>Learners could refer to the following resources:</p> <p>Cisco's Computer Security Incident Response Team (CSIRT) - An overview of CSIRT.</p> <p>Web page https://tools.cisco.com/security/center/emergency.x?i=56#3</p> <p>CSIRT Monitoring for the Cisco House at the London 2012 Olympics Games</p> <p>A video that presents a discussion of cyber security and the London 2012 Olympics Games. http://www.youtube.com/watch?v=Hx8iGQIJ-aQ</p>	1 hour	Unit 3 LO3

Title of suggested activity	Suggested activities	Suggested timings	Also related to
	<p>A video that presents a discussion of cyber security and the London 2012 Olympics Games. http://www.youtube.com/watch?v=Hx8iGQIJ-aQ</p> <p>Cisco's Playbook</p> <p>Web page https://blogs.cisco.com/security/using-a-playbook-model-to-organize-your-information-security-monitoring-strategy/</p> <p>Using a Playbook Model to Organize Your Information Security Monitoring Strategy.</p> <p>CREST: Cyber Security Incident Response - an overview of how to respond to a cyber security incident.</p> <p>A pdf document https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf</p> <p>Incident response and management - an overview of incident and response management.</p> <p>Web page http://www.sans.org/critical-security-controls/control/18</p> <p>Learners could present their work in the form of a report, an information leaflet or a presentation.</p>		
<p>How to respond to a cyber security incident at a work place</p>	<p>Tutors could begin by introducing learners to the different procedures that should be followed in the event of a cyber security incident.</p> <p>Learners could be tasked to document how they would respond to a cyber security incident that happened at a workplace.</p> <p>Learners could refer to the following resources:</p> <p>Cisco's Computer Security Incident Response Team (CSIRT) - An overview of CSIRT.</p> <p>Web page https://tools.cisco.com/security/center/emergency.x?i=56#3</p> <p>CSIRT Monitoring for the Cisco House at the London 2012 Olympics Games</p> <p>A video that presents a discussion of cyber security and the London 2012 Olympics Games. http://www.youtube.com/watch?v=Hx8iGQIJ-aQ</p>	1 hour	Unit 3 LO3



Title of suggested activity	Suggested activities	Suggested timings	Also related to
	<p>Cisco's Playbook</p> <p>Web page https://blogs.cisco.com/security/using-a-playbook-model-to-organize-your-information-security-monitoring-strategy/</p> <p>Using a 'Playbook' Model to Organize Your Information Security Monitoring Strategy</p> <p>CREST has produced the Cyber Security Incident Response Guide – an overview of how to respond to a cyber security incident.</p> <p>A pdf document https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf</p> <p>Incident response and management – an overview of incident and response management.</p> <p>Web page http://www.sans.org/critical-security-controls/control/18</p> <p>Learners could present their work in the form of a report, an information leaflet or a presentation.</p>		
<p>How to produce a cyber security incident report for a cyber security at a work place.</p> 	<p>Tutors could begin by introducing the various stages of investigation that should be undertaken and documented when producing a cyber security incident report.</p> <p>Learners could be presented with a cyber security scenario in a workplace. Learners could then be tasked with investigating the incident and producing a cyber security incident report that documents details of the incident.</p> <p>Learners could refer to the following resource:</p> <p>2014 Cyber Security Session 24 – Cyber Security Incident Response – an overview of how to respond to a cyber security incident.</p> <p>A video (39 minutes) https://www.youtube.com/watch?v=gAb8G0Poj5Y</p>	1 hour	Unit 3 LO3

Title of suggested activity	Suggested activities	Suggested timings	Also related to
<p>How to investigate a cyber security incident at a work place and document the details</p> 	<p>Tutors could begin by introducing the various stages of investigation that should be undertaken and documented when producing a cyber security incident report.</p> <p>Learners could be tasked to produce a guide that teaches members of staff at an organisation how to investigate a cyber security incident.</p> <p>Learners could refer to the following resource:</p> <p>2014 Cyber Security Session 24 – Cyber Security Incident Response – an overview of how to respond to a cyber security incident.</p> <p>A video (39 minutes) https://www.youtube.com/watch?v=gAb8G0Poj5Y</p>	1 hour	Unit 3 LO3

RELATED ACTIVITIES

The Suggested Activities in this Delivery Guide listed below have also been related to other Cambridge Technicals in IT units/Learning Outcomes (LOs). This could help with delivery planning and enable learners to cover multiple parts of units.

This unit (Unit 3)	Title of suggested activity	Other units/LOs	
LO1	Confidentiality, integrity and availability of digital systems	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security LO3 Understand measures used to protect against cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks LO2 Be able to plan computer networks to meet client requirements LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
		Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes
		The importance of keeping data secure	Unit 2 Global information
	Unit 3 Cyber security		LO2 Understand the issues surrounding cyber security LO3 Understand measures used to protect against cyber security incidents LO4 Understand how to manage cyber security incidents
	Unit 4 Computer networks		LO1 Understand the concept of networks LO2 Be able to plan computer networks to meet client requirements LO3 Be able to present network solutions to clients
	Unit 7 Data analysis and design		LO2 Be able to investigate client requirements for data analysis
	Unit 11 Systems analysis and design		LO2 Be able to use investigative techniques to establish requirements for business systems

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO1	The importance of keeping data secure - continued	Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Types of cyber security incidents	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
Unit 21 Web design and prototyping		LO1 Understand the fundamentals of web design	
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	Weaknesses that leave a digital system vulnerable to attack	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
	Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems	
	Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design	
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	The types of threats that digital systems face	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
Unit 4 Computer networks		LO1 Understand the concept of networks	
		LO2 Be able to plan computer networks to meet client requirements	
Unit 7 Data analysis and design		LO2 Be able to investigate client requirements for data analysis	
Unit 11 Systems analysis and design		LO2 Be able to use investigative techniques to establish requirements for business systems	

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	The types of threats that digital systems face - continued	Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Types of attacks to digital systems	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
LO2 Be able to implement software installations and upgrades to meet specified user requirements			

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	Types of attacks to digital systems - continued	Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
		Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes
	Types of malware	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
LO2 Be able to implement software installations and upgrades to meet specified user requirements			
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		
Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	Don't go phishing!	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose		
	LO2 Be able to implement software installations and upgrades to meet specified user requirements		
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		
Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	A rogues' gallery	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO3 Understand measures used to protect against cyber security incidents
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
	LO2 Be able to implement software installations and upgrades to meet specified user requirements		
	Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems	
	Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design	
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Why digital systems are attacked	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO4 Understand how to manage cyber security incidents
Unit 4 Computer networks		LO1 Understand the concept of networks	
		LO2 Be able to plan computer networks to meet client requirements	
	LO3 Be able to present network solutions to clients		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	Why digital systems are attacked - continued	Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Is hacking ever ethical?	Unit 3 Cyber security	LO1 Understand what is meant by cyber security
	Should emails be monitored?	Unit 3 Cyber security	LO1 Understand what is meant by cyber security
	Legal requirements	Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO3 Understand measures used to protect against cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
Unit 11 Systems analysis and design		LO2 Be able to use investigative techniques to establish requirements for business systems	
Unit 12 Mobile technology	LO1 Understand mobile technologies		
Unit 17 Internet of everything	LO2 Be able to repurpose technologies to extend the scope of the IoE		
Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO2	Legal requirements - continued	Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
		Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes
LO3	Identifying assets	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security
			LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose		
	LO2 Be able to implement software installations and upgrades to meet specified user requirements		
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		
Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design		
	LO2 Be able to plan the development of an interactive website for an identified client		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs		
L03	Identifying risks	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems	
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information LO6 Understand the principles of information security	
		Unit 3 Cyber security	LO1 Understand what is meant by cyber security LO2 Understand the issues surrounding cyber security LO4 Understand how to manage cyber security incidents	
		Unit 4 Computer networks	LO1 Understand the concept of networks LO2 Be able to plan computer networks to meet client requirements LO3 Be able to present network solutions to clients	
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis	
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems	
		Unit 12 Mobile technology	LO1 Understand mobile technologies	
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements	
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose LO2 Be able to implement software installations and upgrades to meet specified user requirements	
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems	
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design LO2 Be able to plan the development of an interactive website for an identified client	
		Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
		Testing and monitoring digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
			Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information LO6 Understand the principles of information security
	Unit 3 Cyber security		LO1 Understand what is meant by cyber security LO2 Understand the issues surrounding cyber security LO4 Understand how to manage cyber security incidents	

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
L03	Testing and monitoring digital systems - continued	Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
	Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design	
		LO2 Be able to plan the development of an interactive website for an identified client	
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Physical controls that can be used to secure digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
LO3 Be able to present network solutions to clients			
Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis		
Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems		
Unit 12 Mobile technology	LO1 Understand mobile technologies		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Physical controls that can be used to secure digital systems - continued	Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
			LO2 Be able to plan the development of an interactive website for an identified client
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Hardware control used to secure digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
Unit 21 Web design and prototyping		LO1 Understand the fundamentals of web design	
	LO2 Be able to plan the development of an interactive website for an identified client		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Software controls used secure digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
LO2 Be able to implement software installations and upgrades to meet specified user requirements			
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		
Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design		
	LO2 Be able to plan the development of an interactive website for an identified client		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Data controls used to secure digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
LO2 Be able to implement software installations and upgrades to meet specified user requirements			
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		
Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design		
	LO2 Be able to plan the development of an interactive website for an identified client		
Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Encryption controls used to secure digital systems	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
	Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems	
	Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design	
		LO2 Be able to plan the development of an interactive website for an identified client	
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Controls that are required for personal devices	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
LO4 Understand how to manage cyber security incidents			
Unit 4 Computer networks		LO1 Understand the concept of networks	
	LO2 Be able to plan computer networks to meet client requirements		
	LO3 Be able to present network solutions to clients		
Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Controls that are required for personal devices - continued	Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
		Unit 18 Computer systems – hardware	LO2 Be able to propose a computer system for identified business requirements
		Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose
			LO2 Be able to implement software installations and upgrades to meet specified user requirements
		Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems
		Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design
			LO2 Be able to plan the development of an interactive website for an identified client
	Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes	
	Procedures to keep data secure	Unit 1 Building positive relationships in health and social	LO5 Understand ethical and operational issues and threats to computer systems
		Unit 2 Global information	LO4 Understand the legal and regulatory framework governing the storage and use of global information
			LO6 Understand the principles of information security
		Unit 3 Cyber security	LO2 Understand the issues surrounding cyber security
			LO4 Understand how to manage cyber security incidents
		Unit 4 Computer networks	LO1 Understand the concept of networks
			LO2 Be able to plan computer networks to meet client requirements
			LO3 Be able to present network solutions to clients
		Unit 7 Data analysis and design	LO2 Be able to investigate client requirements for data analysis
		Unit 11 Systems analysis and design	LO2 Be able to use investigative techniques to establish requirements for business systems
		Unit 12 Mobile technology	LO1 Understand mobile technologies
Unit 18 Computer systems – hardware		LO2 Be able to propose a computer system for identified business requirements	
Unit 19 Computer systems – software	LO1 Understand different software installations and their purpose		
	LO2 Be able to implement software installations and upgrades to meet specified user requirements		
Unit 20 IT technical support	LO2 Be able to diagnose faults and solutions for computer systems		

This unit (Unit 4)	Title of suggested activity	Other units/LOs	
LO3	Procedures to keep data secure - continued	Unit 21 Web design and prototyping	LO1 Understand the fundamentals of web design LO2 Be able to plan the development of an interactive website for an identified client
		Unit 22 Big data analytics	LO2 Be able to process Big Data for business purposes
LO4	How to respond to a cyber security incident at home	Unit 3 Cyber security	LO3 Understand measures used to protect against cyber security incidents
	How to respond to a cyber security incident at school/college		
	How to respond to a cyber security incident at work		
	How to produce a cyber security incident report for a cyber security incident at a work place		
	How to investigate a cyber security incident at a work place and document the details		



We'd like to know your view on the resources we produce. By clicking on the 'Like' or 'Dislike' button you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

Whether you already offer OCR qualifications, are new to OCR, or are considering switching from your current provider/awarding organisation, you can request more information by completing the Expression of Interest form which can be found here: www.ocr.org.uk/expression-of-interest

OCR Resources: *the small print*

OCR's resources are provided to support the delivery of OCR qualifications, but in no way constitute an endorsed teaching method that is required by OCR. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources. We update our resources on a regular basis, so please check the OCR website to ensure you have the most up to date version.

This resource may be freely copied and distributed, as long as the OCR logo and this small print remain intact and OCR is acknowledged as the originator of this work.

OCR acknowledges the use of the following content:
Cover image: ra2studio/Shutterstock.com
Square down and Square up: alexwhite/Shutterstock.com

Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk

Looking for a resource?

There is now a quick and easy search tool to help find **free** resources for your qualification:
www.ocr.org.uk/i-want-to/find-resources/

ocr.org.uk/it

OCR Customer Contact Centre

General qualifications

Telephone 01223 553998

Facsimile 01223 552627

Email general.qualifications@ocr.org.uk

OCR is part of Cambridge Assessment, a department of the University of Cambridge. *For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored.*

© **OCR 2018** Oxford Cambridge and RSA Examinations is a Company Limited by Guarantee. Registered in England. Registered office 1 Hills Road, Cambridge CB1 2EU. Registered company number 3484466. OCR is an exempt charity.



Cambridge
Assessment



ISO 9001

001