Unit 40: Principles of ICT Systems and Data Security

Unit code: R/601/3509

QCF Level 3: BTEC Specialist

Credit value: 9

Guided learning hours: 75

Aim and purpose

This unit develops an understanding of the types of threat to ICT systems and data and methods of protecting against them. It also covers an understanding of the applications of cryptography to ICT systems and data.

Unit introduction

Ensuring the security of computer systems and, crucially, the information they store is vital. Organisations and customers require confidence in these matters and security is critical to the successful deployment and use of IT.

In this unit learners will consider physical security of computer systems from simple locks to complex biometric checks, as well as software-based security using, for example, passwords, access rights and encryption.

Potential threats to security arise in different ways. For example, security problems are sometimes related directly to malicious intent from internal or external sources, but in other circumstances such as software piracy, problems can occur by accident or unknowingly. The advent of e-commerce brought with it a whole new set of potential threats and issues for organisations to deal with.

Successful completion of this unit will ensure that all learners and new entrants to the IT industry understand the underlying principles of systems security, as well as developing the knowledge to apply these principles to ensure the security of systems they will be using. Specific technologies, risks and preventative measures are considered, including cryptography.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

On completion of this unit a learner should:

Learning outcomes	Assessment criteria
1 Understand the common types of threat to ICT systems and data	1.1 describe common types of physical threats to ICT systems and data (hardware damage, loss and theft) 1.2 describe common types of electronic threats to ICT systems and data (hardware damage, loss and theft) 1.3 explain the security vulnerabilities associated with remote access technologies (including wireless)
2 Understand how to protect ICT systems	2.1 describe methods of providing physical access control and security for ICT systems (locks, biometric controls, CCTV, shielding, fire detection and control) 2.2 describe methods of providing electronic access control and security for ICT systems (firewalls, virtual networks, secure connection/transfer protocols, secure wireless connection) 2.3 differentiate the following access control methods • mandatory • discretionary • role based 2.4 describe the operation of common types of malicious code: • virus • Trojan • logic bomb • worm • spyware 2.5 describe the characteristics of strong passwords and methods of attacking password-protected systems

Learning outcomes	Assessment criteria
3 Understand the applications of cryptography to ICT systems and data	3.1 describe cryptographic algorithms: • hashing • symmetric • asymmetric 3.2 describe how cryptography can be applied to ICT system and data security in terms of: • confidentiality • integrity • authentication • non-repudiation • access control 3.3 explain the operation of Public Key Infrastructure (PKI) 3.4 explain the concepts of the key management and certificate lifecycles

Unit content

1 Understand the common types of threat to ICT systems and data

Physical threats: damage to hardware eg deliberate or accidental; misuse of equipment eg wrongly set up printer; abuse of equipment eg drink spills; electrostatic discharge (ESD) damage; loss or theft due to easy portability of devices

Electronic threats: weak external security on LAN (Local Area Network); unauthorised access eg by using someone else's username/password; poorly protected passwords; hackers; denial of service attacks; weak external security on LAN eg firewall, web server, mail server, wireless LAN; failure to install network system security updates; counterfeit goods eg software, DVDs, games, music; distribution mechanisms eg boot sales, peer-to-peer networks

Remote access threats: email/internet access eg corrupted email attachment, infected email attachments, corrupted internet downloads, access to malicious websites website defacement; viruses eg rootkits, worms, Trojans; spyware; adware; phishing, identity theft; wireless vulnerabilities eg unsecured wireless access points, VPN (Virtual Private Network)

2 Understand how to protect ICT systems

Physical security: hardware and peripheral security eg locks, visitors passes, sign in/out systems, biometrics eg retinal scans, fingerprint, voice recognition; CCTV (closed-circuit television); shielding eg cable screening, Faraday cages; fire control systems eg detectors, sprinklers

Electronic access controls and security: password protection; strong passwords; access rights and permissions; patch management; application security; virus and spyware protection software; securing mail and web servers; diskless networks; virtual networks; network connection and transfer protocols eg PPTP, TLS, L2 TP, IPSec; secure wireless connections; audit logs; firewall configuration; intruder detection systems; disaster recovery eg backup systems, whole system replacement, tiers of recovery

Access control methods: mandatory, discretionary, role based

Malicious code: how it operates eg virus, Trojan, logic bomb, worm, spyware; attacking passwords

Strong passwords: mixing uppercase, lowercase, numbers, punctuation and other keyboard symbols eg DJ12@ip6#; creating eg created from a phrase that a user can memorise (eg first letters of words of favourite film), first line of poem, numbers and letters from currency note

3 Understand the applications of cryptography to ICT systems and data

Cryptography: encryption and decryption of data; system security; algorithms; eg hashing, symmetric, asymmetric systems application eg confidentiality, integrity, authentication, non-repudiation, access control

Public Key Infrastructure: public keys; certificate authority; trusted third parties; implementation eg Windows Active Directory Certificate Services, Novell Certificate Server; commercial managed solutions eg Verisign, GlobalSign; examples eg encryption and authentication of emails and documents, authentication of users, setting up secure communication channels

PKI management: lifecycle of keys; certification lifecycle

Essential guidance for tutors

Delivery

Visits and talks by external staff are recommended. Access to current magazines and journals would be valuable to keep the content and examples up to date.

To start with, the unit should focus on the common types of threat to IT systems. The tutor could initiate discussions to find out learners' perceptions of IT security and introduce the subject using recent examples of IT systems breaches that have been in the news, such as the loss/theft of important information from government databases and large companies. Learners will be familiar with virus attacks and will probably have heard of many of the types of virus currently 'live' but may not be familiar with other ways networks can be attacked. Useful research about the threats can be carried out using the internet and trade magazines and newspapers. Threats can be discussed and categorised by type and severity.

For learning outcome 1, learners could be taught about different kinds of threats separately, with emphasis placed on where those threats come from. The different nature of the damage caused by these threats could be discussed. It is important for learners to realise how much damage can be done to IT systems, and the subsequent impact it has on businesses.

There are many methods of protecting systems and the unit content gives examples. New devices and software are constantly being produced and it is suggested that a selection of the examples is chosen to concentrate on, ensuring that each of the subtitles under learning outcome 2 is represented. Technical support staff from a local business may be able to give a talk about the security measures they use. Otherwise, case studies can be used.

Cryptography has an interesting history and learners could investigate how cryptography has developed before its application in computing. For learning outcome 3 learners could look at the implementation of a PKI on, for example, a Windows system including the issuing of digital certificates and the use of digital signatures for securing email communication. They could further investigate how a company such as Verisign operates in producing managed PKI solutions.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the programme of suggested assignments. The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to the unit
• Threats to IT systems – research, examples, discussions • Physical threats/electronic threats/remote access threats – categorising, research, examples, external speaker, video.
Protecting systems • Physical security – tutor led, research, video/DVD, external speaker • Electronic security - tutor led, research, video/DVD, external speaker • Access control methods – tutor led, examples • Malicious code – research, discussion • Strong passwords – examples, practical.
Assignment 1 - Threats and how to prevent them
Cryptography • Encryption systems – tutor led, historical research • PKI – tutor led, research.
Assignment 2 - Cryptography!

Assessment

It is suggested that this unit is assessed using the two assignments summarised in the *Programme of suggested assignments* table.

Assignment 1

The evidence for learning outcomes 1 and 2 could be presented as a set of information leaflets. These learning outcomes can be combined to produce a chart(s) or table(s) showing types of threat (1.1 and 1.2) and how to protect against them (2.1 and 2.2).

2.3 to 2.5 can be covered with separate sections covering remote access technologies, access control methods, malicious code and passwords. Apart from 1.3, which requires an explanation of security vulnerabilities, all these criteria require descriptions only.

Any suitable alternative method of producing evidence may be used.

Assignment 2

The evidence for learning outcome 3 could be produced as a presentation. An introduction could explain what cryptography is and how it is applied to data security (3.2). For 3.3 the operation of PKI could be explained using a real-world example and explaining why key management and certificate lifecycles are finite.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the assessment criteria in the assessment and grading grid. This is for guidance and it is recommended that centres either write their own assignments or adapt any Edexcel assignments to meet local needs and resources.

Criteria covered	Assignment title	Scenario	Assessment method
1.1, 1.2, 1.3 2.1, 2.2, 2.3, 2.4, 2.5	Threats and how to prevent them!	You are to produce a set of information leaflets describing the types of threats to computer systems and how to guard against them.	Information leaflets.
3.1, 3.2, 3.3, 3.4	Cryptography!	You are to generate a presentation on cryptography and PKI.	Presentation.

Links to National Occupational Standards, other BTEC units, other BTEC qualifications and other relevant units and qualifications

This unit forms part of the BTEC in IT sector suite. This unit has particular links with:

Level 1	Level 2	Level 3
	Principles of ICT Systems and Data Security	

This unit maps to some of the underpinning knowledge from the following areas of competence in the Level 2 National Occupational Standards for IT (ProCom):

6.1 Information Management
6.2 IT Security Management.

Essential resources

Learners will need access to practical resources and suitable technology. They can also use simulators or multimedia tools to gain experience before handling 'live resources'.

It is essential that learners work in an environment that does not allow them to access system critical resources.

Employer engagement and vocational contexts

Using a local internet service provider engaging in a 'structured' discussion with the ICT network management of your centre.

There is a range of organisations that may be able help centres to engage and involve local employers in the delivery of this unit, for example:

- Learning and Skills Network – www.vocationallearning.org.uk
- Local, regional business links – www.businesslink.gov.uk
- National Education and Business Partnership Network – www.nebpn.org
- Network for Science, Technology, Engineering and Maths Network Ambassadors Scheme – www.stemnet.org.uk
- Work-based learning guidance – www.aimhighersw.ac.uk/wbl.htm
- Work experience/workplace learning frameworks – Centre for Education and Industry (CEI University of Warwick) – www.warwick.ac.uk/wie/cei

Textbooks

Alexander D, Finch A, Sutton D, Taylor A – *Information Security Management Principles: An ISEB Certificate* (British Computer Society, 2008) ISBN 978-1-902505-90-9

Mcillwraith A – *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness* (Gower Publishing Ltd, 2006) ISBN 0566086476

Osborne M – *How to Cheat at Managing Information Security* (Syngress, 2006) ISBN 1597491101

Websites

www.businesslink.gov.uk/bdotg/action/layer?topicId=1075423257

www.cert.org/tech_tips/home_networks.html#III-B-5

Functional Skills – Level 2

Skill	When learners are …
ICT - Using ICT	
Plan solutions to complex tasks by analysing the necessary stages	identifying common types of physical threats to ICT systems and data identifying common types of electronic threats to ICT systems and data identifying methods of providing physical access control and security for ICT systems
ICT - Finding and selecting information	
Use appropriate search techniques to locate and select relevant information	stating how cryptography can be applied to ICT system and data security stating how public key infrastructure operates
ICT - Developing, presenting and communicating information	
Combine and present information in ways that are fit for purpose and audience	identifying security threats to ICT systems and data.