# Unit 14: Principles of ICT Systems and Data Security

**Unit code:** L/601/3508

**QCF Level 2:** BTEC Specialist

**Credit value:** 6

**Guided learning hours:** 45

## Aim and purpose

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

## Unit introduction

Individuals and organisations need to be confident that IT systems are reliable and secure. This is particularly important in such activities as emailing, internet purchases, online services and instant data retrieval. Where this cannot be relied on then the whole use of IT systems is undermined.

Security should not unnecessarily impede access or effective use. Breaches in security may be caused by human actions, either accidentally or by malicious intent, negligence or through incorrect installation, configuration or operation.

In this unit learners will explore ways of maintaining the integrity of IT systems by controlling and monitoring physical access, protecting hardware and protecting data by, for example, encryption. This requires knowledge of both physical and access control security and their application in a real-world situation.

Attacks against computer-based systems are commonplace and increasing and therefore the IT practitioner needs to develop skills to be able to combat such threats. This unit enables learners to understand why security is necessary, the potential dangers, and how to protect systems and data.

## 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 Know the common types of threat to ICT systems and data | 1.1 identify common types of physical threats to ICT systems and data (hardware damage, loss and theft)<br>1.2 identify common types of electronic threats to ICT systems and data (eg denial of service, data theft or damage, unauthorised use)<br>1.3 list the security vulnerabilities associated with remote access technologies (including wireless) |
| 2 Know how to protect ICT systems | 2.1 identify methods of providing physical access control and security for ICT systems (locks, biometric controls, CCTV, shielding, fire detection and control)<br>2.2 state methods of providing electronic access control and security for ICT systems (firewalls, virtual networks, secure connection/transfer protocols, secure wireless connection)<br>• identify common types of malicious code:<br>• virus<br>• trojan<br>• logic bomb<br>• worm<br>• spyware<br>2.3 identify the characteristics of strong passwords |
| 3 Be aware of the applications of cryptography to ICT systems and data | 3.1 state how cryptography can be applied to ICT system and data security<br>3.2 state how Public Key Infrastructure (PKI) operates |

## Unit content

### 1 Know 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

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 Know how to protect ICT systems

Physical security: hardware and peripheral security eg locks, biometric controls, 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; application security; firewalls; virus and spyware protection software; securing mail and web servers; diskless networks; virtual networks; network protocols; secure wireless connections; back up and restore procedures

Malicious code: malware; eg virus, Trojan, logic bomb, worm, spyware

Strong passwords: mixing uppercase, lowercase, numbers, punctuation and other keyboard symbols eg PJW79@ip6#; creating eg created from a phrase that a user can memorise (first letters of words of favourite film), first line of poem, numbers and letters from currency note

### 3 Be aware of the applications of cryptography to ICT systems and data

Cryptography: encryption and decryption of data; encryption systems eg symmetric, public key; applications eg encryption and authentication of emails and documents, authentication of users, setting up secure communication channels

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

## Essential guidance for tutors

### Delivery

Talks by external practitioners and technical support staff could be a useful way of enabling learners to understand the security issues that relate to different business needs and technologies.

The nature of IT security threats is changing constantly, as is the UK and international legislation designed to combat them. To take this into account tutors should try to remain up to date with the latest IT security news, and add this information to the unit as appropriate.

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, for example 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.

Having identified the threats the next step, for learning outcome 2, is to identify how to protect against them. Physical barriers and electronic methods should both be investigated.

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.

## 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<br>• Physical threats/electronic threats/remote access threats – categorising, research, examples, external speaker, video |
| **Protecting systems**<br>• Physical security – tutor led, research, video/DVD, external speaker<br>• Electronic security - tutor led, research, video/DVD, external speaker<br>• Strong passwords – examples, practical |
| **Assignment 1** - Threats and how to prevent them |
| **Cryptography**<br>• Encryption systems – tutor led, historical research<br>• PKI – tutor led, research |
| **Assignment 2** - Cryptography! |

### Assessment

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

**Assignment 1**

Learning outcomes 1 and 2 can be combined and learners can produce a chart(s) or table(s) showing types of threat and how to protect against them. Lists and short descriptions are all that are required.

**Assignment 2**

The evidence for learning outcome 3 could be produced as a leaflet. Different systems of encryption should be included showing where they are used, particular reference should be made to PKI.

**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 |
|---|---|---|---|
| 1.1–1.3, 2.1–2.4 | Threats and how to prevent them! | You are to produce wall charts outlining the types of threats to computer systems and how to guard against them. | Wall charts. |
| 3.1, 3.2 | Cryptography! | You are to produce a leaflet outlining encryption systems, including PKI. | Leaflet. |

**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 (ISP) engaging in a 'structured' discussion with the ICT network management of your centre.

There is a range of organisations that may be able to 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

## Indicative reading for learners

### 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<br>identifying common types of electronic threats to ICT systems and data<br>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<br>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. |