Unit 7: Organisational Systems Security

Unit code: T/601/7312

QCF Level 3: BTEC Nationals

Credit value: 10

Guided learning hours: 60

Aim and purpose

The aim of this unit is to enable learners to understand potential threats to IT systems and the organisational issues related to IT security, and know how to keep systems and data secure from these threats.

Unit introduction

Ensuring the security of computer systems and, crucially, the information they need 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, as well as organisational issues, constraints and policies that impact security, along with legislation specifically relating to computer use.

Security measures are usually in place to serve and protect our privacy and our rights. Security procedures can threaten these rights, for instance the right to have private email. The trade off between security and freedom raises important ethical issues and this unit allows learners to consider ethical decisions and how they can be managed effectively in a modern organisation.

Learning outcomes

On completion of this unit a learner should:

1 Understand the impact of potential threats to IT systems

2 Know how organisations can keep systems and data secure

3 Understand the organisational issues affecting the security of IT systems.

Unit content

1 Understand the impact of potential threats to IT systems

Potential threats: malicious damage; threats related to e-commerce; counterfeit goods; technical failures; other eg human error, theft of equipment

Malicious damage: internal; external; access causing damage eg viruses; access without damage; specific examples eg phishing, identity theft, piggybacking, hacking

Threats related to e-commerce: website defacement; control of access to data via third party suppliers; other eg denial of service attacks

Counterfeit goods: products at risk eg software, DVDs, games, music; distribution mechanisms eg boot sales, peer-to-peer networks

Organisational impact: loss of service; loss of business or income eg through loss of customer records; increased costs; poor image

Information security: confidentiality; data integrity; data completeness; access to data

2 Know how an organisation can keep systems and data secure

Physical security: locks; visitors passes; sign in/out systems; biometrics eg retinal scans, fingerprint, voice recognition; others eg guards, cable shielding

Software and network security: encryption techniques eg public and private key; call back; handshaking; diskless networks; use of backups; audit logs; firewall configuration; virus checking software; use of virtual private networks (VPN); intruder detection systems; passwords; levels of access to data; software updating; disaster recovery eg backup systems, whole system replacement, tiers of recovery

3 Understand the organisational issues affecting the security of IT systems

Security policies and guidelines: disaster recovery policies; updating of security procedures; scheduling of security audits; codes of conduct eg email usage policy, internet usage policy, software acquisition, installation policy; surveillance policies; risk management; budget setting

Employment contracts and security: hiring policies; separation of duties; ensuring compliance including disciplinary procedures; training and communicating with staff as to their responsibilities

Laws: legislation eg Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; privacy and compensation requirements of Data Protection Act 1984, 1998, 2000

Copyrights: open source; freeware; shareware; commercial software

Ethical decision making: eg freedom of information versus personal privacy (electoral roll, phone book and street maps put together); permission eg to use photographs or videos, CCTV footage

Professional bodies: organisations eg Business Software Alliance (BSA), Federation Against Software Theft (FAST), British Computing Society (BCS), Association of Computing Machinery (ACM)

Assessment and grading 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 for a pass grade describe the level of achievement required to pass this unit.

Assessment and grading criteria		
To achieve a pass grade the evidence must show that the learner is able to:	**To achieve a merit grade the evidence must show that, in addition to the pass criteria, the learner is able to:**	**To achieve a distinction grade the evidence must show that, in addition to the pass and merit criteria, the learner is able to:**
P1 explain the impact of different types of threat on an organisation [IE2]	**M1** discuss information security	
P2 describe how physical security measures can help keep systems secure		
P3 describe how software and network security can keep systems and data secure	**M2** explain the operation and use of an encryption technique in ensuring security of transmitted information	**D1** discuss different ways of recovering from a disaster
P4 explain the policies and guidelines for managing organisational IT security issues [EP5]		
P5 explain how employment contracts can affect security		
P6 review the laws related to security and privacy of data.	**M3** explain the role of ethical decision making in organisational IT security.	**D2** evaluate the security policies used in an organisation.

PLTS: This summary references where applicable, in the square brackets, the elements of the personal, learning and thinking skills applicable in the pass criteria. It identifies opportunities for learners to demonstrate effective application of the referenced elements of the skills.

Key			
	IE – independent enquirers	RL – reflective learners	SM – self-managers
	CT – creative thinkers	TW – team workers	EP – effective participators

Essential guidance for tutors

Delivery

The outline learning plan (OLP) is designed as a guide and tutors will use knowledge of their learners to adjust order of delivery accordingly.

This unit is lacking in what might be regarded as 'practical work' and to compensate for this a variety of delivery techniques will be employed.

As a non-practical unit, one of the principal tools that the tutor will have to make use of is detailed case studies. These should be as detailed as possible to give learners the best possible feel for the tasks they are working on.

Another extremely useful learning tool would be bringing in outside expertise, especially if the individual in question represents the organisation which is the subject of the case study. The detail they can provide will be invaluable to making the unit feel 'real' to learners, and not just an exercise in classroom learning.

Discussing IT security issues for the delivery centre is a useful starting point and IT technicians would be able to give details about the techniques and procedures they use to deal with potential threats. The centre should have an individual responsible for the policies and procedures related to IT security and getting them involved will be of great value.

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
• whole-class exercise – tutor presentation on how to prevent unauthorised access • whole-class exercise – class discussions with tutor oversight on how far to prepare for disaster recovery • individual exercise – consider case study where information security has been compromised • whole-class exercise – case study of threats related to e-commerce: • directed research – using tutor-provided materials, find out about why counterfeit goods are a threat to some companies • whole-class exercise – tutor presentation on the organisational impact of ICT security failure.
Assignment 1 – Know Your Threats
• directed research – tutor-directed study of physical security on the internet • whole-class exercise – tutor demonstrates or explains latest ideas/technologies used in biometrics • whole-class exercise – use case studies to examine software and network security.
Assignment 2 – Secure Your Threats

Topic and suggested assignments/activities and/assessment
• directed research – tutor-directed search for information about security policies and guidelines for organisations • whole-class exercise – role play of staff training for employment contracts and security • whole-class exercise – tutor presentation using real-life examples of code of conduct • individual exercise – study relevant laws using tutor-provided materials, including copyright • whole-class exercise – group discussions of what learners think ethical decision making means • directed research – use tutor-provided materials to learn about professional bodies.
Assignment 3 – Issues

Assessment

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

The assessment will be more interesting if a specific organisation has been investigated (better still visited) and learners relate all the evidence to that organisation. A detailed case study could also be used.

For P1, learners must explain the impact of different types of threat on an organisation. Each of the types of threat outlined in the content should be considered. Evidence can be presented in any format – a leaflet is suggested in the programme of suggested assignment.

For M1, learners must discuss information security. Each of the areas set out in the unit content should be covered and related to the threats and their impact. This can be an extension of P1.

For P2, learners must describe the physical measures that can be used to keep systems secure. This can be related to a particular organisation but may need to be supplemented with 'suggestions' for other methods that could be deployed to ensure coverage of the unit content.

P3 is similar to P2, but for software and network security features. P2 and P3 can be included as part of a presentation.

M2 requires an explanation of the operation and use of an encryption technique in ensuring security of transmitted information. The suggestion is that this could be evidenced by a presentation alongside the evidence for P3.

D1 requires learners to investigate disaster recovery options and discuss how and when they would be used. This can also from part of the presentation.

For P4, learners must explain the policies and guidelines employed by an organisation to manage IT security issues. Again, the same organisation can be used. A report is the suggested format here but any suitable format may be used.

P5 is about employment contracts and how they can help security and for P6 the legislation related to security and privacy of data is considered. The unit content should guide coverage.

M3 follows on from P6, and asks the learner to think about the ethical dimensions of IT security. The learner should provide evidence that they have given real consideration to the issues involved and come to a decision about how to deal with them.

D2 extends the material produced for M3 and requires the learner to take what they have learned in the rest of the unit as the basis for evaluating the security policies used in an organisation. This too will form part of the presentation in the suggested assignment.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the pass, merit and distinction 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
P1, M1	Know Your Threats	You are a junior at an IT security consultancy. A manager has asked you to write a short guide to IT security threats and their impact on organisations.	Leaflet
P2, P3, M2, D1	Secure Your Threats	You are to give a presentation to an organisation describing how to keep their systems and data secure.	Presentation
P4-P6, M3, D2	Issues	Finally, you have been asked to create a set of materials dealing with organisational issues.	An illustrated report

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 the following unit titles in the IT suite:

Level 2	Level 3	Level 4
Unit 11: IT Security	Unit 32: Networked Systems Security	Unit 46: Network Security
		Unit 48: IT Security Management

This unit maps to some of the underpinning knowledge from the following areas of competence in the Level 3 National Occupational Standards for IT (ProCom):

- 6.2 IT Security Management.

Essential resources

Learners will need access to good case study material and real examples of organisational policies and procedures.

Employer engagement and vocational contexts

Learners will gain most by researching a real organisation either by visiting it or using visiting speakers.

The Information Commissioner's Office produces excellent teaching and learning materials which highlight the need for control over data. These can provide a useful introduction to the need for privacy, a subject's rights, and an organisation's obligations under the Data Protection Act 1998.

Similarly, there are superb reports produced by the Business Software Alliance which show the amounts of software piracy by area and country of the world. The British Computing Society and the Association of Computing Machinery have sections of their sites devoted to ethical conduct and codes of practice which could be used to enrich the teaching and learning experience.

Indicative reading for learners

Textbooks

Beekman G and Quinn M J – *Computer Confluence Complete: and Student CD – 1st international edition* (Pearson Education, 2005) ISBN-10 1405835796, ISBN-13 978-1405835794

Heathcote P – *A Level ICT – revised edition* (Payne Gallway, 2004) ISBN-10 0953249085, ISBN-13 978-0953249084

Websites

www.acm.org	Association of Computing Machinery
www.bcs.org	British Computing Society
www.bsa.org.uk	Business Software Alliance
www.fast.org.uk	Federation Against Software Theft
www.ico.gov.uk	Information Commissioner's Office

Delivery of personal, learning and thinking skills

The table below identifies the opportunities for personal, learning and thinking skills (PLTS) that have been included within the pass assessment criteria of this unit.

Skill	When learners are ...
Independent enquirers	planning and carrying out research to explain the impact of potential threats on organisations
Effective participators	trying to influence others by describing policies and guidelines for managing organisational ICT security issues, negotiating and balancing diverse views to reach workable solutions.

Although PLTS are identified within this unit as an inherent part of the assessment criteria, there are further opportunities to develop a range of PLTS through various approaches to teaching and learning.

Skill	When learners are ...
Effective participators	Identifying ways to bring in ethical decision making in organisational ICT security that would benefit others as well as themselves.

Functional Skills – Level 2

Skill	When learners are ...
ICT – Finding and selecting information	
Use appropriate search techniques to locate and select relevant information	researching into security matters
ICT – Developing, presenting and communicating information	
Combine and present information in ways that are fit for purpose and audience	explaining encryption techniques and ethical decision making.