Unit 7: IT Systems Security and Encryption

Level: **3**

Unit type: **Internal**

Guided learning hours: **90**

Unit in brief

Learners will study IT system security threats and the methods used to protect against them. Learners undertake activities to protect IT systems from security threats, including data encryption.

Unit introduction

Our increasing reliance on computer systems makes us vulnerable to a range of attacks from cyber criminals. On a global scale, some conflicts reveal that IT systems are a now a target. As IT system security defences become more robust, attack methods become more sophisticated. IT professionals require a good understanding of current security threats and of how to apply appropriate protection methods for any given situation. They also need to comply with legal requirements at all times.

In this unit, you will investigate the many different types of security attack, the vulnerabilities that exist and techniques that can be used to defend the IT systems of organisations. Many organisations run complex IT networks and need them to be secure while providing a safe environment for their employees to work, sharing some data and keeping other data private. You will learn about the complexities of configuring and supporting these networks. You will also explore how encryption can be used to protect data. You will plan and apply suitable protection to an IT system and test it to ensure the protection is effective. You will configure an IT system's access control settings to control user access to various IT system resources, including files, folders and printers. Finally, you will review the protection that you have applied to an IT system and consider how effective it might be in defending the system from attack.

It is important that all IT professionals have a good understanding of security issues and how to defend IT systems against increasingly sophisticated attacks. This unit will prepare you for professional practice as well as entry to a higher education programme that contains elements of cyber security.

Learning aims

In this unit you will:

A Understand current IT security threats, information security and the legal requirements affecting the security of IT systems

B Investigate cryptographic techniques and processes used to protect data

C Examine the techniques used to protect an IT system from security threats

D Implement strategies to protect an IT system from security threats.

Summary of unit

Learning aim	Key content areas	Recommended assessment approach
A Understand current IT security threats, information security and the legal requirements affecting the security of IT systems	**A1** Threat types **A2** Computer network-based threats **A3** Information security **A4** Legal requirements **A5** Impact of security breaches	A report explaining different IT security threats, their potential impact on organisations and the principles of information security and why organisations must adhere to legal requirements when considering security. A report explaining the principles and uses of cryptography, and an assessment of the impact of encryption and security protection, in general, on security and legal issues. An evaluation of the effectiveness of different protection techniques.
B Investigate cryptographic techniques and processes used to protect data	**B1** Cryptographic principles **B2** Cryptographic methods **B3** Applications of cryptography	
C Examine the techniques used to protect an IT system from security threats	**C1** Physical security **C2** Policies and procedures **C3** Software-based protection	Detailed testing documentation explaining how protection techniques can help defend an organisation and a plan showing the protection to be applied to a system to meet specific requirements. Annotated photographic/video evidence of protection measures applied to an IT system. Completed review of the protected IT system. Annotated photographic/video evidence of improvements and optimisations being made to an IT system. Written or audio/video recorded justification of planning decisions and an evaluation of the protected IT system. A report evaluating the plan and the protected system against the requirements.
D Implement strategies to protect an IT system from security threats	**D1** Group policies **D2** Anti-malware protection **D3** Firewall configuration **D4** Wireless security **D5** Access control **D6** Testing and reviewing protection applied to an IT system **D7** Skills, knowledge and behaviours	

Content

Learning aim A: Understand current IT security threats, information security and the legal requirements affecting the security of IT systems

A1 Threat types

Current security threats and techniques (which are continually evolving), including:

- internal threats, e.g. employee actions, data theft, accidental loss, unintentional disclosure or damage to data, unsafe practices (use of external flash storage, visiting untrusted websites, downloading/uploading files to/from the internet, users overriding security controls, file sharing apps and bring your own device (BYOD))
- external threats, e.g. data theft, destruction, withholding and/or disruption of systems (by competitors, cyber criminals, governments, terrorists) for political purposes or financial gain
- physical threats, e.g. theft of equipment or data, malicious damage to equipment or data, damage or destruction by fire, flood, terrorist action or other disaster
- social engineering and software-driven threats, techniques used to obtain secure information (software that has a malicious intent), e.g. malware, viruses, worms, Trojan horses, ransomware, spyware, adware, rootkits and backdoors.

A2 Computer network-based threats

- Passive threats, including wiretapping, port scanning and idle scanning.
- Active threats, including denial-of-service attack, spoofing, man in the middle, Address Resolution Protocol (ARP) poisoning, smurf attack, buffer overflow, heap overflow, format string attack, Structured Query Language (SQL) injection and cyber attack.
- Cloud computing security risks.

A3 Information security

- Principles of confidentiality, integrity and availability of information.
- Unauthorised access or modification of information.
- Principle of minimal access to information or lowest required access permission to be able to maximise protection.
- Deliberate or accidental loss of information.
- The need to protect intellectual property from theft or malicious damage, e.g. personal information, bank account details, employment details.

A4 Legal requirements

Legislation must be current and applicable to England, Wales or Northern Ireland, as appropriate to where the qualification is being taught.

- Data Protection Act 1998 and the requirements it places on organisations to keep data about stakeholders secure.
- Computer Misuse Act 1990 and its definitions of illegal practices and applications.
- Copyright, Designs and Patents Act 1988 and its requirements in terms of protecting software products and digital media such as music and films.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and their requirement to allow companies to monitor employee communication using IT systems and other uses of the internet while at work.
- Fraud Act 2006 and its requirement to deal with services using IT-based methods to steal information for fraudulent purposes.
- Legal liability and contractual obligations.

A5 Impact of security breaches

A serious security breach is likely to result in one or more of the following:

- operational impact on an organisation of the loss of data or service
- financial impact of loss of service, such as an e-commerce website
- damage to reputation
- legal consequences of data privacy breaches
- forensics research requirements to identify data lost, stolen or copied.

Learning aim B: Investigate cryptographic techniques and processes used to protect data

B1 Cryptographic principles

- The principles and uses of encryption, including digital rights management (DRM); password storing and salts; obfuscation and steganography; secure transactions; two-factor authentication; file, folder, disk encryption; encryption of communication data, e.g. police, mobile phone.
- Legal and ethical issues.
- Computational hardness assumption.

B2 Cryptography methods

Key cryptography methods, e.g.:

- shift ciphers, one-time pads, hash functions (e.g. MD4, MD5, SHA-2 SHA-3), block ciphers, stream ciphers
- cryptographic primitives, e.g. pseudo random functions, one-way functions
- cryptographic salts and their use in storing passwords
- encryption algorithms, e.g. RSA, DES, 3DES
- mathematical principles, integer factorisation, prediction of prime numbers.

B3 Applications of cryptography

The types and application of cryptography, including:

- symmetric key encryption
- public key encryption
- key exchanges (Diffe-Hellman)
- digital certificates (including certificate authorities)
- HTTPS protocol
- virtual private networks (VPNs)
- Generic Routing Encapsulation (GRE) tunnels
- encryption of data on Wi-Fi networks.

Learning aim C: Examine the techniques used to protect an IT system from security threats

Protection techniques, to include physical security, policies and procedures, software-based protection and regular audit of security.

C1 Physical security

- Building and computer/network room security, e.g. door locks, card key entry, closed circuit television (CCTV), voice control and biometrics such as facial recognition, fingerprint and iris scans, DNA identification technology.
- Servers, routers, switches kept in a secure location with controlled access.
- Backing up data, e.g. full backup, differential and incremental backups, use of a fire safe and off-site storage of data.
- IT disaster recovery plans for use when an organisation's IT systems become unavailable.

C2 Policies and procedures

Relevant policies and procedures, including:

- organisational policies and their application, including internet and email use policies, security and password procedures, staff responsibilities, training of staff on IT security issues, disciplinary procedures
- security audits and their application to check compliance of policies and procedures
- default 'factory settings' and 'reset' options are removed from hardware and software configuration
- any known backdoors are removed
- management of patches for hardware (firmware) and software (operating systems, security applications)
- installation of applicable security updates, including rollout management, minimising disruption, sandbox testing of updates and establishing potential risks
- any rules created do not impede normal business operation for an individual and the organisation:
  - ingress and egress of expected network traffic
  - server interconnectivity
  - time based, allowing/preventing resource access
  - allowing external access to internal servers
  - allowing data interchange between suppliers, business partners, external cloud-based solutions
  - the impact of aggressive email filters
  - use of different software by different individuals.

C3 Software-based protection

- Anti-virus software and detection techniques, including virus signatures, heuristic techniques used to identify potentially suspicious file content, techniques for dealing with identified threats.
- Software and hardware firewalls and the filtering techniques they use, including packet filtering, inbound and outbound rules, and network address translation.
- Intrusion detection systems (IDSs), including setting signatures, establishing requirements, traffic monitoring.
- Domain management, including prevention of unintended devices joining a system.
- User authentication, including user log-on procedures, strong passwords, text and graphical passwords, biometric authentication, two-step verification, security tokens (e.g. USB-based keys), knowledge-based authentication (e.g. question and response pairs), Kerberos network authentication for Windows® and Linux®-based systems, certificate-based authentication.
- Access controls and the methods they use to restrict authorised/unauthorised users access to resources (user groups and the access rights allocated to them such as folders, files and physical resource such as printers), e.g. Windows NTFS file permissions, Linux octal file permissions.

Learning aim D: Implement strategies to protect an IT system from security threats

D1 Group policies

- Tools for managing a set of IT systems.

D2 Anti-malware protection

- Installation of anti-malware software, configuration of anti-malware scanning schedules.

D3 Firewall configuration

Hardware and/or operating system-embedded firewalls, including configuration of:

- inbound and outbound rules to control network connections that are allowed and prevent all other unauthorised connections
- firewall events and interpretation of log entries.

D4 Wireless security

- Wireless encryption methods, e.g. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2.
- Configuration of wireless router security settings.

D5 Access control

- Design and implementation of hardware and software access control regimes, including permission settings on files, folders and resources.
- Defining legitimate users and groups, and the resources they need to access and the levels of access they need (read, modify, delete).
- Defining password policies, including length, complexity, age and reuse for desktop and server computers.
- White listing of applications' trusted signed binaries.
- Data hiding when viewing logs and visibility of sensitive data.
- Defining users with special privileges, e.g. administrator rights and when these are used.

D6 Testing and reviewing protection applied to an IT system

- Firewall testing to check the firewall blocks unauthorised traffic and allows legitimate traffic through.
- Systematically test 'allowed' and 'blocked' entry points.
- Run system scans of all relevant hardware and software on a secured system using common testing tools.
- Network testing tools, including scanners, security-based operating system distribution, sniffers.
- Viewing and interpreting activity logs.
- Judging the effectiveness of protection and making recommendations for further improvements.

D7 Skills, knowledge and behaviours

- Planning and recording, including the setting of relevant targets with timescales, and how and when feedback from others will be gathered.
- Reviewing and responding to outcomes, including feedback from IT professionals and users, e.g. effectiveness of protection, degree to which the protection hinders the system's everyday use.
- Demonstrate own behaviours and their impact on outcomes, including professionalism, etiquette, being supportive of others, timely and appropriate leadership, accountability.
- Evaluating outcomes to help inform high-quality, justified recommendations and decisions.
- Documenting processes and outcomes, e.g. diary notes, planning documents, witness testimonies and discussion notes or recordings.
- Communication skills, including:
  - conveying intended meaning, e.g. written (email, design documentation, recording documentation, reports, visual aids for use in presentations use); verbal communication requirements (one-to-one and group informal and formal situations)
  - use of tone and language for verbal and written communications to convey intended meaning and make a positive and constructive impact on the audience, e.g. positive and engaging tone, technical/vocational language suitable for intended audience, avoidance of jargon.
  - responding constructively to the contributions of others, e.g. being supportive, managing contributions so all have the opportunity to contribute, responding to objections, managing expectation, resolving conflict.

Assessment criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">Learning aim A: Understand current IT security threats, information security and the legal requirements affecting the security of IT systems</td><td rowspan="4">AB.D1 Evaluate the effectiveness of the techniques used to protect organisations from security threats while taking account of the principles of information security and legal requirements.</td></tr>
<tr><td>A.P1 Explain the different security threats that can affect the IT systems of organisations.
A.P2 Explain the principles of information security when protecting the IT systems of organisations.
A.P3 Explain why organisations must adhere to legal requirements when considering IT systems security.</td><td>A.M1 Assess the impact that IT security threats can have on organisations' IT systems and business while taking account of the principles of information security and legal requirements.</td></tr>
<tr><td colspan="2">Learning aim B: Investigate cryptographic techniques and processes used to protect data</td></tr>
<tr><td>B.P4 Explain the principles and uses of cryptography to secure and protect data.</td><td>B.M2 Analyse how the principles and uses of cryptography impact the security and protection of data.</td></tr>
<tr><td colspan="2">Learning aim C: Examine the techniques used to protect an IT system from security threats</td><td rowspan="4">CD.D2 Evaluate the plan and the effectiveness of the protected IT system against requirements.
CD.D3 Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.</td></tr>
<tr><td>C.P5 Explain how protection techniques can help defend an organisation from security threats.
C.P6 Produce a plan to protect an IT system that meets organisational and legislative requirements.</td><td>C.M3 Justify the choice of protection techniques used to defend the IT systems of an organisation, showing how its IT system will be protected from security threats.</td></tr>
<tr><td colspan="2">Learning aim D: Implement strategies to protect an IT system from security threats</td></tr>
<tr><td>D.P7 Perform tasks to protect the IT system to meet requirements given in the plan.
D.P8 Review the extent to which the organisation's IT system has been protected.</td><td>D.M4 Enhance the protection of the IT system to meet requirements given in the plan.</td></tr>
</table>

Essential information for assignments

The recommended structure of assessment is shown in the unit summary with suitable forms of evidence. *Section 6* gives information on setting assignments and there is further information on our website.

There is a maximum number of two summative assignments for this unit. The relationship of the learning aims and criteria is:

Learning aims: A and B (A.P1, A.P2, A.P3, B.P4, A.M1, B.M2, AB.D1)

Learning aims: C and D (C.P5, C.P6, D.P7, D.P8, C.M3, D.M4, CD.D2, CD.D3)

Further information for teachers and assessors

Resource requirements

As IT security is a very fast-moving discipline, regular research will be needed to keep learning delivery up to date – for example any changes to legislation applicable to IT security and the protection of IT systems and organisations.

For this unit, learners must have access to hardware and software resources that will allow them to apply security protection measures. Examples include computer systems, laptops or a virtualised environment, providing that they do not compromise the security of other 'live' systems. Learners may also need access to networking hardware such as a switch, wireless access point and router.

Essential information for assessment decisions

Learning aims A and B

For distinction standard, learners will provide comprehensive evidence that they have fully investigated and considered how effective security protection measures are likely to be in defending the IT systems of organisations against the security threats that they have been examining. Learners must discuss the protection techniques that are likely to be effective and those that are not, explaining why each technique would or would not be effective. They will make links between the effects of the security threats identified in their investigation, the effectiveness of the protection, the legal requirements (for example to keep personal data secure) and the information security requirements, as listed in the unit content. The evidence will demonstrate high-quality written or oral communication through the use of accurate and fluent technical vocabulary, which supports a well-structured and considered response that clearly connects chains of reasoning.

For merit standard, learners will provide a clear, balanced assessment of the potential impact of a wide range of IT security threats to organisations that rely on IT systems. Learners will refer to real-life examples of how security breaches have impacted on organisations.

Learners must provide a clear, balanced analysis of how the principles and uses of cryptography impact on the security and protection of data. For example, encryption techniques can have different strengths of protection, with the risk that some are more vulnerable than others. The evidence must be technically accurate and demonstrate good-quality written communication.

For pass standard, learners will provide detailed explanations of the various IT security threats, including why IT systems are vulnerable or not, as the case may be. Learners must cover internal, external, physical, social engineering and software threats. They also need to cover the principles of information security and the legal requirements that apply to an organisation's IT systems. For example, learners could explain how access control methods can help organisations comply with data protection and privacy laws and organisational requirements for confidentiality. They could also explain how company IT policies can make it clear to employees that employers have the right to monitor their emails and internet use at work. When covering the principles and uses of cryptography, learners will provide detailed technical explanations. The evidence may have some inaccuracies.

Learning aims C and D

For distinction standard, learners will draw on, and show synthesis of, knowledge across the learning aims to evaluate their plan, measure the effectiveness of the security protection methods applied to the IT system and refer to how their solution met the stated requirements. For example, learners have chosen to apply specific access controls for certain users, they would need to show how effective this measure is in terms of granting access to the right users and preventing access to others. Learners must also include what they have done differently where measures have been ineffective. Evidence must include results of testing carried out on the security that has been applied, as well as a review of planning against the implementation of the protection.

Learners will articulate their arguments and views concisely and professionally, and evaluate concepts, ideas and actions to reach reasoned and valid conclusions when justifying planning and implementing decisions in the protection of an IT system. They will demonstrate individual responsibility for their own work (for example identifying potential issues and resolving these, reviewing their work and making improvements, keeping their work safe and secure and showing responsible use of quoted materials) and effective self-management when planning and applying security protection methods to an IT system, including how they have handled breaches. They can also show awareness of how this is managed by organisations – for example, Product Security Incident Response Teams (PSIRTs). Learners must provide evidence of their methods of working, which can be diary notes, planning documents, witness testimonies, and discussion notes or recordings.

For merit standard, learners will provide a clear, reasoned justification of choices they have made in the planning of the security protection techniques they intend to use. This must include technical reasons why they selected particular protection methods and configurations and rejected others. Learners also need to show that they have carried out tasks that improve the protection provided and minimise the impact of the protection techniques on overall system performance and usability. This could include tasks such as setting scheduled virus scans and updates at appropriate times, adjusting firewall settings to unblock legitimate programs, and adjusting shared folder permissions and password policies to balance protection and convenience.

For pass standard, learners will produce a detailed, realistic plan that clearly shows what they intend to do to protect the IT system from a range of IT security threats. They must provide evidence of implementing the plan on a mock-up or virtualised system. Learners will provide a completed test plan to show that the IT system and its protection have been tested to ensure that the protection is effective and does not hinder the normal use of the system. The system must provide levels of access to folders as required by the organisation. Learners also need to provide evidence that the protected system has been reviewed by others, considering the protection provided and the usability of the system. The evidence could take the form of a written review or a video recorded discussion of the system. Learners must produce a solution that meets the requirements of the plan, although some minor issues may persist.

Links to other units

This unit links to:

- Unit 6: IT Systems Security
- Unit 9: The Impact of Computing
- Unit 19: Computer Networking
- Unit 20: Managing and Supporting Systems
- Unit 29: Network Operating Systems
- Unit 30: Communication Technologies.

Employer involvement

This unit would benefit from employer involvement in the form of:

- guest speakers
- technical workshops involving staff from local organisations/businesses
- contribution of design/ideas to unit assignment/scenario/case study/project materials, including own organisation/business materials as exemplars where appropriate
- feedback from staff from local organisations/businesses on plans/designs/items developed
- opportunities for observation of organisational/business application during work experience
- support from local organisation/business staff as mentors.