Unit 11: Cyber Security and Incident Management

Level: **3**

Unit type: **External**

Guided learning hours: **120**

Unit in brief

Learners study cyber security threats and vulnerabilities, the methods used to protect systems against threats and how to plan for and manage security incidents.

Unit introduction

Our increasing reliance on computer systems and the data they contain makes us vulnerable to attacks from cyber criminals, and also to the loss of these systems if there is an accident or a natural disaster. As IT system security is improved, more sophisticated methods of attack are developed, and it is important that organisations have robust plans in place to deal with a cyber security incident before it occurs. All IT professionals require a good understanding of the current threats to systems, how to apply appropriate and effective protection methods and how to manage a cyber security incident.

In this unit, you will examine the many different types of cyber security attacks, the vulnerabilities that exist in networked systems and the techniques that can be used to defend an organisation's networked systems. You will investigate the techniques used to assess risks and ways of planning to deal with the results of a cyber security incident and recover systems following an incident. You will examine scenarios, carry out risk assessments and prepare protection plans before protecting networked systems. You will also examine evidence from cyber security incidents and relevant security documentation, using the evidence to make recommendations for improvement. To complete the assessment tasks within this unit, you will need to draw on your learning from across your programme.

As IT systems evolve, there is an increasing need for IT professionals to protect networked systems and the information they contain, while providing enhanced features and benefits for organisations, customers and individuals. This unit will help prepare you for IT courses in higher education and for technician-level roles and apprenticeships in a variety of related areas.

Summary of assessment

This unit is externally assessed by a task set and marked by Pearson. The set task will be completed under supervised conditions in sessions: Part A is five hours and Part B is four hours. Part A must be completed before Part B and both parts need to be completed during the three-week assessment period set by Pearson.

The set task will assess learners' ability to design appropriate cyber security measures for networked systems and to analyse a security incident.

The number of marks for the unit is 80. The tasks will be marked using a levels-based mark scheme that is located in the sample assessment materials.

The availability of the task is December/January and May/June each year. The first assessment availability is May/June 2018.

Sample assessment materials will be available to help centres prepare learners for assessment.

Assessment outcomes

AO1 Demonstrate knowledge and understanding of technical language, security threats, system vulnerabilities and security protection methods, and implications resulting from successful threats

AO2 Apply knowledge and understanding of security threats, system vulnerabilities and security protection methods and implications in order to risk assess systems and select appropriate tools to secure them

AO3 Analyse forensic evidence data and information to identify security breaches and manage security incidents

AO4 Evaluate protection methods and security documentation to make reasoned judgements and draw conclusions about their efficacy

AO5 Be able to plan a secure computer network and manage security incidents with appropriate justification

Essential content

The essential content is set out under content areas. Learners must cover all specified content before the assessment.

A Cyber security threats, system vulnerabilities and security protection methods

A1 Cyber security threats

All systems are vulnerable to attack from external and internal threats.

- Understand how internal threats occur, including:
  - employee sabotage and theft, including of physical equipment or data, and damage such as fire, flood, power loss, terrorism or other disaster
  - unauthorised access by employees and other users to secure areas and administration functions, including security levels and protocols
  - weak cyber security measures and unsafe practices, including security of computer equipment and storage devices, security vetting of visitors, visiting untrustworthy websites
  - accidental loss or disclosure of data, including poor staff training and monitoring.
- Understand how external threats function, including:
  - malicious software (malware), including spyware, adware, ransomware; viruses, including worms, rootkits and trojans
  - hacking, including commercial, government, individuals
  - sabotage, including commercial, government, terrorism, individuals
  - social-engineering techniques used to obtain secure information by deception.
- Understand that the impact of a credible threat is likely to result in some form of loss, such as:
  - operational loss, including manufacturing output, service availability and service data
  - financial loss, including organisational, compensation and legal liability
  - reputation loss, including lack of service and employee or customer information
  - intellectual property loss, including new product design or trade secret.
- Understand that the impact level of a successful attack on an organisation is determined by the value of the loss, and that the value may not always be a monetary one.
- Know that cyber security threats vary over time and cyber security organisations provide regular updates on the current and changing threat landscape.

A2 System vulnerabilities

- Understand that different types of computer and/or system are exposed to different threats and that they contain different vulnerabilities. Possible vulnerabilities include:
  - network, including firewall ports and external storage devices
  - organisational, including file permissions or privileges, password policy
  - software, including from an untrustworthy source, downloaded software, illegal copies, SQL injection and new zero-day exploits
  - operating system, including unsupported versions, updates not installed
  - mobile devices reliant on Original Equipment Manufacturers (OEMs) to update system software
  - physical, including theft of equipment, Universal Serial Bus (USB) storage devices with sensitive data, collection of passwords and other information by social-engineering methods
  - process of how people use the system, including leaks and sharing security details
  - security implications of cloud computing and of the Internet of Things (IoT) devices.
- Understand where to find up-to-date sources of information on specific known hardware and software vulnerabilities.
- Attack vectors, including: Wi-Fi, Bluetooth®, internet connection, internal network access.

A3 Legal responsibilities

Understand how the current and relevant European Union (EU) General Data Protection Regulation (GDPR) and United Kingdom legislation or other international equivalents apply to different systems, including:

- Data protection legislation and amendments, requirements for organisations to keep data secure
- Computer Misuse Act 1990 and amendments, its definitions of illegal practices and applications
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and amendments, requirements to allow companies to monitor an employee's communication and internet use while at work
- Fraud Act 2006 and amendments, requirements to deal with services using IT-based methods to steal information for fraudulent purposes
- Health and Safety at Work etc. Act 1974 – duties of employers, employees, the Health and Safety Executive (HSE) and others, general prohibitions.

A4 Physical security measures

Understand the use and effectiveness of physical security measures, including:

- site security locks, card entry, biometrics, closed-circuit television (CCTV), security staff, alarms, protected cabling and cabinets
- data storage, data protection and backup procedures, including planned automated backup, on- and off-site data storage and cloud storage.

A5 Software and hardware security measures

- Understand the use and effectiveness of software and hardware security measures, including:
  - antivirus software and detection techniques, including virus signatures, heuristics 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 and inspection
    - application layer awareness
    - inbound and outbound rules
    - network address
  - user authentication:
    - user login procedures
    - strong password
    - text and graphical password
    - biometric authentication
    - two-step verification
    - security tokens, including USB-based and near field keys
    - knowledge-based authentication, including question and response pairs
    - Kerberos network authentication for Windows® and Linux®-based operating systems
    - certificate-based authentication
  - access controls and the methods to restrict users' access to resources, including applications, folders, files and physical resources
  - trusted computing.
- Understand the purpose and uses of encryption, including:
  - safe password storage
  - digital rights management (DRM)
  - file, folder, disc encryption

  - communications encryption:
    - built into devices, including smartphones and tablets
    - The Onion Router (Tor)
    - virtual private networks (VPNs)
    - digital certificates and certificate authorities
    - Hypertext Transfer Protocol Secure (HTTPS)
    - public/private keys.
- Precautions that can be taken to protect a wireless local area network (WLAN) from unauthorised access, including:
  - MAC address filtering and hiding the service set identifier (SSID)
  - wireless encryption – Wired Equivalent Privacy (WEP), Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Setup (WPS), mitigating known wireless vulnerabilities
  - consideration of security issues during network and system design to ensure security is built-in from the development stage.

B Use of networking architectures and principles for security

Understand the security implications of different networked systems, including how to secure them in organisational contexts.

B1 Network types

- Applications and features of networks:
  - local area network (LAN), WLAN, wide area network (WAN), storage area network (SAN), personal area network (PAN)
  - intranet, extranet, internet, cloud
  - wired and wireless integration.
- Applications and features of network topologies:
  - physical topologies, including star, extended star, hierarchical, wireless mesh, ad-hoc (mix of wired and wireless for bring your own device (BYOD))
  - logical topologies, including Ethernet standards for wired and wireless (802 family).
- Applications and features of network architecture:
  - peer to peer
  - client/server
  - thin client.
- Modern trends, including applications and features of: virtualisation, cloud computing, BYOD, software-defined networking (SDN), storage-defined networks and the IoT.
- Be able to interpret and amend network schematic diagrams using suitable software.

B2 Network components

- Application and features of hardware components, including:
  - end-user devices, including mobile
  - connectivity devices, including switches, routers, access points, multi-functional devices, USB hubs and modems
  - connection media, including cable, wireless (Wi-Fi, Bluetooth, and infrared (IR)), fibre and Li-Fi.
- Applications and features of external media and storage, including flash drives and optical media.
- Applications and features of software components, including:
  - network and device operating systems
  - network monitoring, management and troubleshooting tools, including performance monitor, events and logs viewer, vulnerability scanners and packet sniffers
  - network applications, including database, document management and network discovery tools.

B3 Networking infrastructure services and resources

- Understand the application and function of:
  - Transmission Control Protocol/Internet Protocol (TCP/IP)
  - ports
  - packets
  - network address translation (NAT), including the structure of IPv4 and IPv6 addressing and RFC 1918 private addresses.
- Understand the application of network operating systems, including domains and sub-domains.
- Understand the application of network devices to configure networks, including network segmentation.
- Understand the function and application of network infrastructure services, including:
  - domain name system (DNS)
  - directory services (DS), including active directory, open directory, OpenLDAP
  - authentication services
  - Dynamic Host Configuration Protocol (DHCP)
  - routing
  - remote access services.
- Understand the function and application network services and resources:
  - file and print services
  - web, mail and communications services.

C Cyber security protection plan

Understand that as threats and system vulnerabilities are constant and ever changing, a culture of continuous improvement is needed to protect organisations and individuals from the impact of loss.

C1 Assessment of computer system vulnerabilities

Understand that:

- the types and uses of tools and methods to assess the vulnerabilities in computer systems, including port scanners, registry checker, website vulnerability scanners, vulnerability detection and management software, and assessing user vulnerabilities
- the purpose of independent third-party review of a system and network designs before implementation
- the applications and features of penetration testing for common threats, those in the Open Web Application Security Project (OWASP) top 10.

C2 Assessment of the risk severity for each threat

- A risk is a threat that could result in some form of loss at some point in time.
- Risk severity = probability of the threat occurring × expected impact level/value of the loss.
- Measures for risk severity include:
  - risk severity = low, medium, high and extreme
  - probability of the threat occurring = unlikely (approximately every year), likely (approximately every week or month) and very likely (approximately once or more a day)
  - impact level/value of the loss = minor, moderate and major.
- Be able to use the following risk severity matrix:

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Impact level/value of the loss			

- Risk assessment approach:
  - risk assessments are carried out during system design (review) and at regular intervals during operation (audit) and following a security breach, as threats are constant and ever changing
  - a risk assessment method:
    - identify possible threats and assess the probability of different threats occurring
    - assess the vulnerabilities of a computer-networked system to specific threats
    - assess the impact level/value of the potential loss
    - determine the risk severity (low, medium, high and extreme).

C3 A cyber security plan for a system

A plan for a networked system, including:

- cyber security protection measures to be taken (actions) for the most severe (medium, high and extreme) risks with the largest impact level/loss value and that are most likely to occur, to include:
  - hardware protection measures, including firewalls, routers, wireless access points
  - software protection measures, including anti-malware, firewall, port scanning, access rights and information availability
  - physical protection measures, including locks, CCTV, alarms, data storage and backups
  - alternative risk management measures, including risk transfer to a third party (commissioning a service provider), risk avoidance by stopping an activity and risk acceptance
- a justification about how each planned protection measure would protect the system from attack
- an overview of any technical and financial constraints
- an overview of legal responsibilities
- an overview of usability of the system, including the degree to which security restrictions impact on the efficiency of the system in terms of the ease of completing tasks and the user experience
- outline cost–benefit analysis of implementing the protection measures
- test plan to check that the protection measures work as intended, including the test description, expected outcome, and possible further action following the test.

D Cyber security documentation

Understand the governance policies and documents needed to establish and maintain security on an ongoing basis.

D1 Internal policies

General IT policies

- The purpose and content of general security-related IT policies and their effectiveness, including:
  - understanding the requirements to prepare a cyber security policy using the Plan-Do-Check-Act loop derived from part of the International Organization for Standardization (ISO) 27001:2013
  - organisation policies and their application, including policies on internet and email use, security and password procedures, staff responsibilities, staff IT security training
  - security audits and their application to check compliance against policies
  - backup policy – selection of data, methods (full and incremental), frequency and storage
  - data protection policy – to ensure organisational compliance with the relevant legislation.

Incident response policy

- The purpose and content of an incident response policy and associated procedures:
  - assembling the Computer Security Incident Response Team (CSIRT), roles in the team, including team leader, incident lead, associate members
  - incident reporting procedures, including what constitutes a security incident, and how to report it and to whom
  - initial assessment of the incident, including identifying if this is a real incident, the type of attack and its severity
  - communicating the incident to the CSIRT and other relevant individuals
  - containing the damage and minimising the risk
  - protect people's safety:
    - protect sensitive data and other data, protecting the most valuable first
    - protect hardware and software
    - minimise disruption to computing resources
  - identifying the type and severity of the compromise, including the nature of the attack, its intent, its origin and the systems and files that have been compromised
  - protecting evidence and creating backups for evidence and data recovery, including the removal and storage of original hard disks
  - notifying external agencies, if appropriate, and discussing options with legal representatives, contact external agencies such as law enforcement, external security and virus experts
  - recovery of systems and identification of the point in time when the compromise occurred and restore backups from before that point in time
  - compile and organise incident documentation, including documentation created by the CSIRT identifying the details of the breach and actions taken
  - know the importance of preserving and collating documentation that may be needed to prosecute offenders
  - review outcomes to update policies and improve training.

Disaster recovery policy

- Understand the topics typically covered in a disaster recovery plan and their purpose:
  - identification of critical systems, definitions of recovery time objective (RTO) and recovery point objective (RPO)
  - prevention, response and recovery strategies for critical systems, including:
    - people responsible
    - facilities and equipment required
    - data backup location and format
    - network connectivity and bandwidth
    - suppliers of equipment and people
  - definition of recovery procedures for each critical system
  - disaster recovery plan structure following ISO 27031/24762 or other relevant international equivalents, including:
    - introduction
    - roles and responsibilities
    - incident response procedures
    - activating the disaster recovery plan
    - procedures to be followed.

D2 External service providers

- External service provider (ESP) agreements will include:
  - cloud
  - hardware
  - software.
- Understand the implications of ESP agreements, including:
  - legal ownership and jurisdiction, including geographical location, data movement across borders, procedures when an agreement ends

  - security protection, including data security obligations, privacy, encryption, liability for data breaches, liability for data loss or damage (accidental or deliberate), disaster recovery procedures
  - dispute resolution, including statutory requirements, and problems encountered by data and processing residing in multiple jurisdictions.
- Many or all of these points are covered by the data protection laws.

E Forensic procedures

E1 Forensic collection of evidence

Understand the forensic collection of evidence following a security incident and its purpose:

- desktop forensics:
  - meeting requirements for desktop forensics, including:
    - confiscation of devices
    - taking an image of the system
    - using a forensic analysis tool
    - reviewing files and settings
    - reviewing system logs
    - reviewing user activity
    - malware analysis and alerts
  - the challenges of live forensics:
    - changing data in situ
    - recovering corrupted data and preventing data corruption
    - capturing data in active memory
    - losing temporary files
- network forensics:
  - agreeing a network-testing methodology with forensic supervisory and investigatory authority
  - scanning of local infrastructure:
    - ensuring permission is granted
    - ensuring that testing protocol will not disrupt a live system
    - passive and active analysis tools
  - reviewing and analysing firewalls, infrastructure devices, including switch, router, wireless access point, client or server logs
  - analysing malware activity and alerts.

E2 Systematic forensic analysis of a suspect system

- Requirements for maintaining an accurate record, made at the time, or as soon after the incident as possible.
- Retaining snapshots of the system.
- Requirements for the recording of all findings and considering how reliable the evidence is.
- Requirements for the recording of any alterations that have been intentionally and unintentionally imposed by the investigator.
- Requirements for the creation of visual evidence of findings.
- Ensuring the evidence is relevant and not a false positive.
- Evaluation of the findings to determine whether or not they:
  - provide evidence of a crime and/or an incident
  - show that the system has been externally and/or internally compromised
  - strongly support one possible cause more than other possible causes.
- Make recommendations to prevent security incidents from reoccurring in the future, including improvement(s) to the:
  - content of cyber security documentation (policies and/or agreements)
  - adherence of cyber security documentation (policies and/or agreements)
  - security protection measures (physical, software and/or hardware).

Grade descriptors

To achieve a grade learners are expected to demonstrate these attributes across the essential content of the unit. The principle of best fit will apply in awarding grades.

Level 3 Pass

Learners are able to apply their knowledge and understanding of cyber security in unfamiliar scenarios in order to identify common risks and use familiar security protection measures to improve the security of an existing networked system. They can give adequate justification for some aspects of their design. Learners can design tests for basic security procedures.

Learners are able to analyse straightforward forensic evidence related to security incidents to produce plausible conclusions. They are able to identify common security weaknesses in a given scenario and suggest improvements.

Learners will use some appropriate technical language to communicate their ideas.

Level 3 Distinction

Learners are able to apply knowledge and understanding of cyber security in unfamiliar scenarios in order to identify common and uncommon risks and use a range of security protection measures to comprehensively secure an existing networked system. They can give a valid and supported justification for their design. Learners can design tests for a range of security procedures.

Learners are able to analyse more complex forensic evidence related to security incidents to produce coherent and convincing conclusions together with alternative possibilities. They are able to identify a range of security weaknesses in a given scenario and make valid, realistic and justified suggestions for improvement.

Learners will use appropriate technical language consistently to communicate their ideas.

Key words typically used in assessment

The following table shows the key words that will be used consistently by Pearson in our assessments to ensure learners are rewarded for demonstrating the necessary skills.

Please note: the list below will not necessarily be used in every paper/session and is provided for guidance only.

Command or term	Definition
Anti-malware software	A software program that attempts to identify and neutralise software that has a malicious intent (malware) on a system.
Cloud computing	Using software and/or hardware resources that are operated by a third party remotely.
Cyber security plan	A plan that describes threats, protection measures (actions), reasons for the measures, constraints, legal responsibilities, usability, cost/benefit and a test plan.
Domain	An administrative division of a client/server network.
Firewall	A software or hardware device that monitors incoming and outgoing network traffic, applying rules to allow or disallow certain types of traffic.

Command or term	Definition
Hacker	A person who attempts to gain unauthorised access to a system using methods referred to as 'hacking'.
Risk assessment	A document that identifies the security risks to a system and determines the likelihood of each risk occurring and the severity of the loss that may occur as a result of an incident.
Security incident management policy	A document that defines how an organisation will respond to an IT security incident.
Security requirements	Security needs of a networked system, either specified by the client or implied by the scenario.
Service provider agreement	A document that a service provider uses to define a variety of aspects of an IT service provided, including security requirements.

Links to other units

The assessment for this unit should draw on knowledge, understanding and skills developed from:

- Unit 1: Information Technology Systems
- Unit 2: Creating Systems to Manage Information
- Unit 3: Using Social Media in Business
- Unit 4: Programming
- Unit 9: IT Project Management.

This unit would relate to teaching of:

- Unit 13: Software Testing
- Unit 16: Cloud Storage and Collaboration Tools
- Unit 21: Business Process Modelling Tools.

Employer involvement

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

- work shadowing opportunities for learners to observe security issues first-hand
- guest speakers to explain organisation security policies and procedures
- technical workshops hosted by local organisations covering security procedures (e.g. configuring firewalls, file/folder permissions etc.).

Please note that some organisations may be reluctant to provide too much information about their security procedures.