Unit 11: Cyber Security and Incident Management

Delivery guidance

As modern life becomes increasingly reliant on computer systems and the data they store, process and transmit, the battle to keep IT systems secure in the face of external threats, accidents and natural disasters becomes ever more challenging.

This unit presents learners with the highly topical and challenging experience of studying cyber security threats and vulnerabilities, the methods used to protect systems and how to plan for, investigate and manage potentially devastating security incidents.

Progressive cyber security and incident management rely on five core skills:

- understanding different networking architectures and how to secure them
- knowing cyber security threats and system vulnerabilities and security
- assessing the level of risk and the recovery methods available
- knowing how to collect evidence from a suspect system using forensically sound methods
- designing comprehensive and detailed cyber security plans.

This unit will give learners a sound foundation in security and computer forensic disciplines for higher education. If the class or course has a virtual learning environment (VLE), this is a good way for learners to share some of their documented outcomes, as recommended in this guide and in the scheme of work.

Approaching the unit

Although this unit contains a considerable amount of theoretical content, it should be taught in an active fashion using targeted practical activities, particularly with regard to security and network-related concepts. This delivery guide recommends the use of pre-prepared disk images which contain the necessary resources or system 'snapshots' and offer the advantage of reusability.

Where possible, all technologies used (hardware or software – see the Resources section for examples) should be open source projects or freeware. Case studies and reference material relating to current threats, vulnerabilities and protection methods should be as current as possible. The use of regularly updated (and searchable) online databases is highly recommended.

If possible, provide learner access to quarantined network facilities and open source software. This will help learners to simulate, detect, investigate and manage many different types of cyber security threat in a safe environment, giving an insight into the real-world dangers they pose in a controlled and observable manner.

Newly-discovered system vulnerabilities and devastating cyber security attacks frequently appear in news headlines, so collect and use examples as real-world case studies. This will help to ground and contextualise the concepts, bringing technically austere material to life in exciting ways.

Delivering the learning aims

Learning aim A requires learners to demonstrate knowledge and understanding of technical language, security threats, system vulnerabilities, legal implications and security protection methods. Teach the investigation of different cyber security threats by exploring each type of threat and linking it with a real-world example, where the personal, financial, operational, reputational, legal or criminal impacts are clear for learners to see. This will reinforce the severity of each threat in learners' minds. Use various approaches to help learners understand how external threats function, for example, there are many online videos which illustrate how malware (malicious software) works or discuss how to successfully hack a website or use social-engineering techniques. You could also use socially-active ethical hackers or system administrators to act as guest speakers.

System vulnerabilities are best tackled by exploring each category in turn (network, organisational, software, operating system, etc.) and selecting particular exploits that can be replicated by learners. Practical examples could include:

- deliberately infecting a target machine on a quarantine network with an infected download
- performing an SQL injection on a locally hosted web application
- accessing administrative web interfaces on Internet of Things (IoT) devices such as webcams via default passwords.

Encourage learners to explore up-to-date sources of information for known hardware and software vulnerabilities to exploit (under suitable supervision). Demonstrate more traditional forms of vulnerability (e.g. theft of portable hardware) by considering appropriate physical security measures designed to mitigate these vulnerabilities, such as security locks, CCTV and protected cabling.

The specific legislation linked with this unit may be covered elsewhere but, traditionally, it is best taught through research and presentation. Other techniques (such as court-based role plays using case studies) may offer a viable and more active approach.

Ensure learners understand relevant legislation in their own country and appreciate that legislation may be different around the world. They should also understand that there is an expectation in other countries that their legislation will be observed in addition to local requirements.

Complete this content area by revisiting the threats and vulnerabilities identified earlier and demonstrating the software and hardware measures that can provide protection against them. This content is best delivered through demonstration, using a round robin of practical activities which learners can try individually, in pairs or in small groups. Good examples include:

- encryption and decryption of data
- disinfecting malware from computer systems
- installing and configuring firewalls to block bad network traffic
- improving user authentication
- changing user permissions
- enabling MAC filtering and wireless encryption
- hardening server-side scripts to filter SQL injections.

This approach will allow learners to associate each potential threat with a practical solution, which will be beneficial for part A of the externally set task.

Learning aim B requires learners to have a working knowledge of different networking architectures, different services and their functions, and how to secure them in organisational contexts.

Networks are the core target of many cyber security threats, with their continued operation and robustness against internal and external threats playing a key role in the practicability of an organisation's day-to-day operations.

You should essentially split this content area into three parts, focusing on:

- the network types
- the network components used
- the typical resources and services a network provides.

Networking topics such as types (LANs, WANs, SANs, etc.) and their physical and logical topologies and adherent standards (e.g. 802 family, etc.) are well-documented, with a wealth of reference texts, video tutorials and websites available for learner use (see the Resources section for examples). Directed research is often the best way to teach this content but there are alternatives, such as investigating a 'volunteer' network infrastructure to identify its type, topologies and standards. This could form part of an organised industrial visit.

Teach the coverage of network components in a practical manner, combining as many hands-on network building activities as possible, including the use of different types of end-user device, connectivity device and media type. The assembly of a small quarantine network is ideal, as this network can then be used as a platform for the installation and use of network applications, components and resources. Where physical kit and space are limited, the use of virtual network design and visualisation tools (such as Cisco Packet Tracer) is highly recommended.

Explore network infrastructure and services through presentations and demonstrations, supplemented by online videos and animations that detail their working (see the Resources section). If possible, use a quarantine network to enable learners to set up a DNS server, configure a DHCP service and populate typical directory services (DS). It will be rewarding for the learner to both configure the DHCP address pool on a server and change a networked client to obtain its IP address from a dynamic DHCP request rather than using a static address; this approach will also make the process transparent and easy to understand. Try to demystify services and resources in this way, including shared services (files and printers), web hosting and internal email. If physical resources are limited, network visualisation tools (such as the Cisco Network Simulator) support simulated services and offer a viable alternative; open source simulators are also available, such as Cloonix and Mininet.

Note that many networking concepts involve the use of different number bases, including (but not limited to) binary, octal and hexadecimal, so there are several opportunities to reinforce numeracy in this topic. It is also a good idea to link security concepts with network infrastructure and services – for example, when demonstrating or configuring DHCP on a wireless network, emphasise that the assignment of an IP address could rely on the client device's MAC address being successfully filtered. This will help learners to make links between the two topics, in preparation for part A of the externally set task.

Learning aim C requires learners to:

- assess risk vulnerabilities and the levels of risk attached to those vulnerabilities
- evaluate protection methods
- develop security plans which make reasoned judgements
- draw conclusions about the efficacy of those plans.

Broadly speaking, this content area can be separated into three parts: assessing computer vulnerabilities, assessing the risk severity for each threat identified and creating a cyber security plan for a given system.

To assess a computer system's vulnerabilities, learners must have access to quarantined systems that they can interrogate, as well as a range of software tools (for which they will require formal instruction and time to become proficient). Activities such as port scanning a test server are easily accomplished and there are several command-line and GUI-based utilities that can perform this task. (Command-line tools should be used where possible, as this will reinforce learners' reliance on Microsoft Windows and GUI-based utilities.) The Open Web Application Security Project (OWASP) Top 10 provides a good reference list of popular exploits: make learners aware of this list and allow them to study some of these exploits as case studies.

Use deliberately vulnerable web applications (particularly those involving poorly-written PHP) to allow learners to explore the impact and risks of poor programming. Encourage learners to exploit the application 'as is' from a web client, then amend the application's source code on the server using OWASP recommendations, before trying to exploit the application again (hopefully unsuccessfully). Performing such 'real world' vulnerability fixes is good preparation for the type of thinking required when creating a cyber security protection plan.

For any identified threat, learners must calculate the risk severity using the recommended matrix (see unit content), which balances threat probability with impact level/value of loss incurred. Cover this process by working through a set of threats and asking learners to decide, by applying the risk severity matrix, how urgently an appropriate protection measure can be selected and applied. Use moderated group discussion, perhaps collating findings from smaller working parties (each with their own identified threat to rate) to enhance learners' understanding of this process.

It will be difficult for learners to produce a cyber security plan for a system without having seen a model paper. You can simply present a checklist of content expected in such a plan (e.g. software and hardware protection measures, risk assessment, constraints, legal responsibilities, etc.); however, it will be far more revealing to examine an existing document and ask learners to identify its different features. From here, it should be possible to ask learners to construct a document for a selected case study (after they have investigated, identified the vulnerabilities and assessed their risks).

For this learning aim, learners must understand governance policies and documents needed to establish and maintain security on an ongoing basis. You will need to present a number of different policies including ISO 27001:2013, typical organisation policies and policies that enforce relevant local legislation, e.g. Data Protection legislation.

Governance policies, international standards and organisation-level policies can feel very remote if they are not grounded within learners' everyday experience of IT systems and processes. Make links with policies learners will have encountered, such as:

- IT policies relating to the required complexity of user passwords
- backup of learner data
- acceptable use of email and the internet.

The challenge here is to ask learners to think more like a technician trying to secure a system than a user who may resent the limitations placed on their user experience by such policies.

In addition, various forms of relevant legislation are covered in other units on the programme, so integration with these units is a useful learning tactic.

Other areas of focus should include incident response and disaster recovery policies. The content list in the specification is very thorough and is best delivered through small case studies, role-play activities (e.g. how to report an incident correctly) and key documents for review and discussion. Group discussion is a useful technique for debating the pros and cons of a particular response to a given incident.

Finally, introduce the role of the external service provider (ESP). You may be able to find local companies who fulfil ESP roles (e.g. hosting and data warehousing) to discuss (in general terms) the types of agreements they establish with their clients. Moderate a prepared question-and-answer session on these agreements to identify any gaps in coverage that need to be addressed, particularly with regard to dispute resolution, etc.

Learning aim D requires learners to analyse forensic evidence data and information to identify security breaches and manage security incidents.

Forensic computing principles rely on strict processes and recordkeeping, particularly in terms of keeping a chain of evidence. (Tutors must ensure delivery covers local arrangements.) Focus on the professional characteristics required for this type of task – thoughtfulness, diligence and good organisation.

Use a popular Linux distribution to teach new practical skills, such as:

- cloning a file system
- checking recently mounted devices
- showing recent firewall activity
- viewing configuration files
- scanning a system for operating security holes, network or application vulnerabilities.

Many open source and freeware forensic tools for Linux-based operating systems can be downloaded from reputable websites, to enable these activities. Guest speakers, perhaps from the institution's own network infrastructure and services team, can also provide additional insight.

At every stage, ensure learners understand that they must observe the challenges of live forensics – the need to work in situ, the ability to recover deleted files or read encrypted ones, dumping the contents of live RAM to disk – all while avoiding the loss of temporary files that may contain vital information.

The use of a live case study, with model procedures, is perhaps the best way to deliver this content area, allowing learners to investigate a realistic scenario and gather evidence using recommended tools and techniques in a controlled environment. Learners should ideally work in pairs or small groups as this can stimulate lively discussion and rationalisation of their findings to make appropriate judgements and recommendations. The case study may take the form of a hacked server with deliberate footprints of the intruder's actions logged and discoverable; the presence of suspect files, recently deleted files, doctored log files, amended databases or configuration changes are easy to manufacture. Removal of existing protection or deliberate creation of 'flawed' security settings are also obvious 'clues' that can be engineered.

Equip learners with a range of tools and techniques that will allow them to investigate, find and – most importantly – record the evidence they need without damaging or changing it. Note: As part of their external assessment, learners will be required to complete a forensic incident analysis based on unseen evidence. Provide appropriate recording tools (electronic or paper-based), along with examples of similar cyber security documentation (policies and procedures) that learners can use to recommend revised security protection measures, based on the evaluation of their forensic findings.

Assessment model

Learning aim	Key content areas	Recommended assessment approach
A Understand cyber security threats, system vulnerabilities and security protection measures	**A1** Cyber security threats **A2** System vulnerabilities **A3** Legal responsibilities **A4** Physical security measures **A5** Software and hardware security measures	This unit will be assessed using a set assignment brief provided by Pearson. Learners will be required to respond to a Pearson Set Assignment Brief, which will provide a scenario detailing the specific organisation. Learners will produce formal reports that contain: ● an exploration of cyber security threats and how an organisation can implement security measures to counteract these ● an assessment of organisation network types and their vulnerabilities ● an implementation plan and evaluation of a cyber security plan for a specified organisation.
B Explore the security implications of networked systems	**B1** Network types **B2** Network components **B3** Networking infrastructure services and resources	
C Develop a cyber security protection plan for a specified organisation	**C1** Assessment of computer system vulnerabilities **C2** Assessment of the risk severity for each threat **C3** A cyber security plan for a system **C4** Internal policies **C5** External service providers	
D Examine procedures to collect forensic evidence following a security incident	**D1** Forensic collection of evidence **D2** Systematic forensic analysis of a suspect system	

Assessment guidance

The assessment for this unit will be externally set by Pearson, internally assessed by tutors and externally moderated, using the external standards verification process common to BTEC units. It will consist of a single assignment undertaken under controlled conditions.

Learners are permitted to re-sit assignments during their programme. (For more information, please see the specification.)

Assignments are available from September each year and are valid for one year only.

Getting started

This gives you a starting point for one way of delivering the unit, based around the recommended assessment approach in the specification.

Unit 11: Cyber Security and Incident Management

Introduction

Introduce this unit by ascertaining learners' experience with security issues and vulnerabilities; they may have experienced denial of access to products and services due to system outages caused by cyberattacks or internal failures. Reference local current events, such as:

- Netherlands: Maastricht University paid €250 000 to ransomware hackers (Jan 2020)
- Jordan: Jordan leaps upward in Global Cybersecurity Index ranking (Jul 2019)
- Pakistan: Understanding Pakistan's cybersecurity woes (Mar 2019)
- Turkey: Cyberattacks blamed for Sunday's internet disruption across Turkey (Oct 2019)
- UAE: Is the UAE at risk due to cyber security skills shortage? (Jan 2019)

Ask how many day-to-day activities involve computers, particularly those that store, process and communicate valuable, private or critical data. Share statistics – such as the number of probes and hacking attempts a typical website receives each day – to highlight the scale of the problem faced by IT security professionals.

Where possible, teach this unit in a practical manner; although there is a considerable amount of theoretical knowledge for learners to engage with (particularly in terms of correct business processes and legislation), the key to securing a computer system (or forensically investigating one) is the ability to select and use the necessary tools and techniques appropriately.

You could also appoint (or asking for volunteer) learners with more networking or operating system experience – particularly with Linux distributions – to provide classroom support.

Learning aim A: Understand cyber security threats, system vulnerabilities and security protection methods

A1: Cyber security threats

- Detail different types of cyber security threat, differentiating between internal and external threats.
- Give a presentation, including sample case studies and examples, to show how internal threats occur, e.g. sabotage, theft, natural disaster (flood, etc.), unauthorised access, system vulnerabilities, unsafe practices, etc.
- Give a presentation, including sample case studies and examples, to show how external threats occur, e.g. malicious software (different types), hacking (individual, commercial and government sponsored), sabotage and social engineering.
- Lead a group discussion incorporating learners' own experiences, e.g. leaked passwords, compromised accounts, Sony emails and account hack, Xbox Live DoS attacks, etc.
- Ask learners to investigate selected case studies which focus on the impact (operational, financial, reputational or intellectual loss) of a threat or vulnerability which has been exploited. This can be used later in risk assessments.
- Ask learners to suggest how organisations can keep abreast of changing cyber security threats and protect their operations and data.
- A template for a cyber security plan can be found on the Pearson website. It is highly recommended that this is used to ensure complete coverage of the requirements.

A2: System vulnerabilities

- Detail different types of system vulnerability.
- Give a presentation, with supporting practical demonstrations, of different types of system vulnerability, for example, a badly configured firewall, poorly selected file permissions or user privileges, weak password policy, etc.
- Demonstrate the dangers posed by software applications. You could do this by downloading an infected application from an untrusted source onto a quarantined PC and observing the impact, or by performing an SQL injection attack on an insecure web application, etc.
- Discuss topical examples, e.g. botnets utilising weak security on IoT (Internet of Things) household devices to perform DDoS (Distributed Denial of Service) attacks.
- Ask learners to research software and hardware vulnerabilities for specific products using appropriate sources, e.g. Common Vulnerabilities and Exposures (CVE) database. Note: If possible, demonstrate well-chosen examples in a controlled network environment.
- Ask learners to create informational posters about common attack vectors, including WiFi, Bluetooth, etc.

A3: Legal responsibilities

- Detail the relevant local legislation that applies to different systems.
- Ask learners to summarise relevant legislation and present their findings to their peers (for example, via a blog, wiki or podcast).
- Consider using the following examples as a basis for research:
    - UAE: *Cybersecurity regulations and their impacts*
    - Jordan: *MPs pass 2019 Cyber Security Law*
    - Netherlands: *Stricter enforcement of cybersecurity rules to be expected in the Netherlands*
    - Turkey: *Getting the deal through – Cybersecurity Turkey*
    - Pakistan: *Cyber Security: Where does Pakistan stand?*
- Lead a discussion that links the different legislation with the ways an organisation (or individual) should respond.
- Compare and contrast local and international legislation, e.g. 2001 USA Patriot Act, 1998 Digital Millennium Copyright Act (DMCA), etc.
- Explore news stories and case studies about prosecutions under local legislation. Encourage learners to consider the impact of internet-based cybercrime on the sovereignty of legal authority.

A4: Physical security measures

- Discuss and demonstrate various physical security measures.
- Learners will be familiar with many common physical security measures such as locks, protected cabling, card entry and closed-circuit television (CCTV). As such, place more emphasis on physical security measures used to secure specific locations, such as hosting companies and data warehouses. If possible, arrange for learners to visit such locations.
- Demonstrate the use of biometric devices to access systems, e.g. unlocking a desktop PC using a fingerprint scanner.
- Discuss physical security measures applied to data storage, data protection and backup procedures.

A5: Software and hardware security measures

- Explore various software and hardware security measures.
- Lead, demonstrate and support practical activities in which learners:
  - install various types of anti-virus software, updating their signatures and selecting appropriate actions to disinfect affected files
  - install and configure a firewall to accept, block, drop or log specific packets of data, depending on various aspects of the transmission (e.g. connection state, source or destination IP, UDP or TCP, port number, etc.)
  - test various login procedures, particularly those with multi-factor authentication; learners should experiment with creating strong passwords and different forms of authentication, including knowledge-based, Kerberos and certificate-based (e.g. SSH public/private key pairs and agent forwarding)
  - change authorisation and user permissions to affect their (and others') access to resources, e.g. folders, files, processes and physical devices.
- Discuss the concept of trusted computing and its key components, e.g. endorsement key, memory curtaining, sealed storage, etc.
- Present basic encryption concepts including how it works (an outline), its objectives and commercial applications. Link each commercial example with a realistic real-world demonstration, e.g. using an HTTPS connection on a website to obscure the transmission of sensitive data such as usernames and passwords on a login.
- Demonstrate how to secure a wireless local area network (WLAN) from unauthorised access, using techniques such as channel changing, MAC address filtering, limited guest networks, SSID broadcast suppression, wireless encryption (WEP, WPA, WPA2, WPS), etc. Note: There are many tutorials on popular video sharing sites that demonstrate the successful reveal of WEP encryption keys. This type of activity can usually be replicated very cheaply (using older hardware and open source software) in a controlled classroom environment. These techniques can be used as an aid in the development of risk assessments.

Learning aim B: Explore the security implications of networked systems

B1: Network types

- Introduce different network types, their topologies, components, services and resources.
- Present the applications and features of networks. Introduce networks in ascending order (e.g. PAN to WAN) and ensure terms such as intranet, extranet, internet and cloud are fully defined and differentiated.
- Discuss physical and logical topologies and ask learners to explore different types, for example, by creating network topology posters.
- Use appropriate media, connections and devices to demonstrate the various standards for wired and wireless connections.
- Differentiate between different network architecture models, including peer to peer, client/server and thin client.
- Using an example, discuss and highlight modern trends in networking, including 'bring your own device' (BYOD), the 'Internet of Things' (IoT) and software-defined networking (SDN).
- Introduce network visualisation tools that will enable learners to create networks and interpret schematic diagrams in an interactive fashion. Cisco Packet Tracer is a good example of this type of application.

B2: Network components

- Demonstrate the different components of a network.
- Allow learners to examine and combine different types of network component, with the aim of creating a simple Local Area Network (LAN).
- Introduce applications and features of external media and storage, including flash drives and optical media.
- Demonstrate the different applications and features of a variety of software components. Ask learners to complete a range of activities, such as:
    - installing and configuring a network operating system
    - using network tools to confirm connectivity or troubleshooting issues
    - using monitoring tools to view network throughput
    - viewing network events and system/device logs
    - sniffing transmitted packets in network traffic using a protocol analyser
    - scanning a network's open ports for vulnerabilities
    - installing and testing network-aware applications such as relational databases by remotely connecting and querying a simple data source.

B3: Networking infrastructure services and resources

- Detail networking infrastructure services and resources.
- Explain the application and function of Transmission Control Protocol/Internet Protocol (TCP/IP), ports, packets and network address translation (NAT), including the structure of IPv4 and IPv6 addressing and RFC 1918 private addresses.
- Use of a protocol analyser to capture incoming and outgoing data packets can be very informative when tracking a simple network operation such as a ping. Learners should be able to use such tools to track packets 'in' and 'out' of their computer, inspect the data being sent and identify the source and destination IP addresses.
- Ask learners to investigate network configuration, including the use of domains and sub-domains.
- Demonstrate different configurations that change the way network devices work, e.g. a router issuing IP addresses via DHCP. Another good example would be using a switch to segment a network using its Virtual Local Area Network (VLAN) functionality.
- Help learners to explore a variety of network infrastructure services, such as:
    - domain name system (DNS)
    - directory services (DS) including Microsoft Windows Active Directory and open source implements such as OpenLDAP
    - authentication services
    - Dynamic Host Configuration Protocol (DHCP)
    - routing
    - remote access services such as Remote Desktop Protocol (RDP) or Secure Shell (SSH).
- Demonstrate the installation, configuration and use of network services and resources including file and print services, web hosting, mail and communication services. For example, enable a web server on a quarantine LAN and access its resources via a client using HTTP request. Show learners how to track the whole HTTP request and response process by viewing these requests using a protocol analyser, inspecting the web server's access log, and finally rendering the transmitted resource on a web browser. Then

demonstrate real-time modifications to the served content by requesting the resource again.

Learning aim C: Develop and cyber security protection plan for a specified organisation

C1: Assessment of computer system vulnerabilities and C2: Assessment of the risk severity for each threat

- Demonstrate how to calculate the risk severity for each threat.
    - Define the risk severity as the probability of the threat occurring multiplied by the expected impact level/value of the loss.
    - Differentiate risks as low, medium, high and extreme. This can link back to earlier topics where risks and exploits were identified.
    - Differentiate the probability of the threat occurring as unlikely, likely or very likely.
    - Differentiate the impact level/value of the loss as minor, moderate or major.
- Ask learners to create a risk severity matrix; this could be a manual diagram, word-processed table, spreadsheet, website form or programmed solution.
- Ask learners to consider a given set of real-world scenarios, assess the probability and impact levels and thus calculate the risk severity. Lead a class discussion to collate their ideas.
- Review risk assessment approach and methods.

C3: A cyber security plan for a system

- Create a cyber security plan for a system.
- Discuss when to plan cyber security measures (based on medium, high and extreme risk severity for identified threats).
- Present a model cyber security plan for a given scenario and walk learners through the various sections, e.g. software and hardware protection measures, risk assessment, constraints, legal responsibilities, etc.
- Separate learners into groups of three or four and ask them to construct a document for a selected case study (after they have investigated, identified the vulnerabilities and assessed their risks). Ensure learners understand that the format of their document should match that of the model plan.
- Note that learners will need to cover the following areas in their assessment:
    - threat(s) addressed by the protection measure
    - details of action(s) to be taken
    - reasons for the actions
    - overview of constraints – technical and financial
    - overview of legal responsibilities
    - overview of usability of the system
    - outline cost–benefit analysis.
- Ask learner groups to swap their plans with their peers and evaluate whether the protection measures would work as intended, identifying good practice and possible areas for improvement.

C4: Internal policies

- Detail the cyber security documentation which needs to be observed, established and maintained by an organisation.
- Present general IT policies, their content and rationale. There are some very good examples of general IT policies on the internet which could be used as a basis for discussion.
- Allow learners to examine your institution's IT policies, such as email and internet use, backup and data protection. You could split learners into groups and give each group a different policy to examine. They should highlight the key points and potential outcomes of non-compliance.
- Discuss and explore incident response policy. Ask local organisations to provide anonymised policies that you can use with learners. Ask learners to compare these policies, to identify differences between the requirements of different organisations or any key omissions.
- Examine at least two real incident reports. These reports should include a range of content as outlined in the specification (such as type and severity of the compromise, nature of attack, its intent and origin, which files were affected, etc.). Make links with learning aim D1, explaining briefly how the evidence relating to these incidents was collected and recorded.
- Discuss and explore disaster response policy. Learners will benefit from a broad approach to this topic, preferably with input from a number of guest speakers or organisations who can give real examples of disaster recovery plans. If possible, contact an organisation which has had to recover from some kind of disaster (e.g. a natural disaster or some kind of serious data loss), to discuss lessons learned.
- There is a range of roles in disaster recovery, so ask any speakers to explain how many people are needed to fulfil these roles. (In some organisations, all the tasks and responsibilities will fall to one person.)

C5: External service providers

- Explore the role of an external service provider (ESP).
- Discuss ESP agreements for cloud services, applications and storage, giving a range of examples across different services.
- Discuss ESP agreements for hardware and software. Allow learners to explore two or three different examples, particularly in relation to maintenance responsibilities.
- Present the implications of ESP agreements, including legal ownership and jurisdiction, security and dispute resolution. Illustrate this content with real-life examples and case studies, considering what can go wrong. This can make a relatively dry topic more interesting, particularly if multiple jurisdictions are involved.
- Ask learners to determine which types of agreement may be covered by data protection laws as relevant to the learner's native country and in relation to trading with international partners.

Learning aim D: Examine procedures to collect forensic evidence following a security incident

D1: Forensic collection of evidence

- Detail the process of collecting evidence after a security incident, using a forensically sound methodology.
- Present desktop forensic activities.
- Lead and support practical sessions to allow learners to develop practical skills, e.g.
    - cloning a file system

  - checking recently mounted devices
  - showing recent firewall activity
  - viewing configuration files
  - scanning a system for operating security holes and network or application vulnerabilities.
- Ask guest speakers, perhaps from the institution's own network infrastructure and services team, to provide additional insight and hold a learner question-and-answer session.
- Discuss the challenges of live forensics.
- Examine the procedures required to perform network forensics.

D2: Systematic forensic analysis of a suspect system

- Detail the systematic forensic analysis of a suspect system.
- Discuss the requirements for maintaining accurate records.
- Present a checklist of different evidence sources and demonstrate how to obtain the required evidence.
- Work through a model forensic report of an incident and ask learners to:
  - evaluate the findings and determine whether or not they prove a crime has been committed
  - show the source of the compromise (internal or external)
  - ascertain whether or not a single cause can be clearly proven.
- Ask learners to produce a report, with recommendations on how to prevent similar security incidents in the future. Learners should draw on security measures they have been taught and they must justify their recommendations.
- Give learners feedback on their recommendations.

Details of links to other BTEC units and qualifications, and to other relevant units/qualifications

This unit links to:

- Unit 1: Information Technology Systems – Strategy, Management and Infrastructure
- Unit 2: Creating Systems to Manage Information
- Unit 3: Using Social Media in Business
- Unit 4: Programming
- Unit 9: IT Project Management
- Unit 13: Software Testing
- Unit 15: Cloud Storage and Collaboration Tools
- Unit 20: Business Process Modelling Tools

Resources

In addition to the resources listed below, publishers are likely to produce Pearson-endorsed textbooks that support this unit of the BTEC Internationals in Information Technology. http://qualifications.pearson.com/endorsed-resources for more information as titles achieve endorsement.

Websites

- *Acunetix Vulnerability Scanner* – An automation tool which examines websites, looking for common vulnerabilities
- *Wireshark* – The world's most commonly-used network protocol analyser
- *Squid-cache* – A caching proxy for the web, supporting HTTP, HTTPS and FTP
- *Cisco Packet Tracer* – A free network simulation and visualisation tool
- *Common Vulnerabilities and Exposures (CVE)* – An online dictionary of common names for publicly-known information security vulnerabilities

Learners should study cyber security legislation in different countries. You could ask them to search online for the following relevant articles:

- UAE: Cybersecurity regulations and their impacts
- Jordan: MPs pass 2019 cyber security law
- Netherlands: Stricter enforcement of cybersecurity rules to be expected in the Netherlands
- Turkey: Getting the deal through – Cybersecurity Turkey
- Pakistan: Cyber Security: Where Does Pakistan Stand?

Videos

You may wish to search YouTube for the following videos:

- *Network Threats: Port Scanning* **–** Part of a series on network threats, this video focuses on port scanning (both for validation of security policy and for vulnerability reconnaissance).
- *Hack All The Things: 20 Devices in 45 Minutes* **–** A really useful lecture revealing 20 device vulnerabilities and how they can be exploited.

- *SQL Injection Basics Demonstration* – A video demonstration of SQL injection techniques to exploit a web application.
- *Vulnerability Assessment and Mitigating Attacks* **–** A good introductory video which gives an overview of these concepts.

Pearson is not responsible for the content of any external internet sites. It is essential for tutors to preview each website before using it in class so as to ensure that the URL is still accurate, relevant and appropriate. We suggest that tutors bookmark useful websites and consider enabling learners to access them through the school/college intranet.