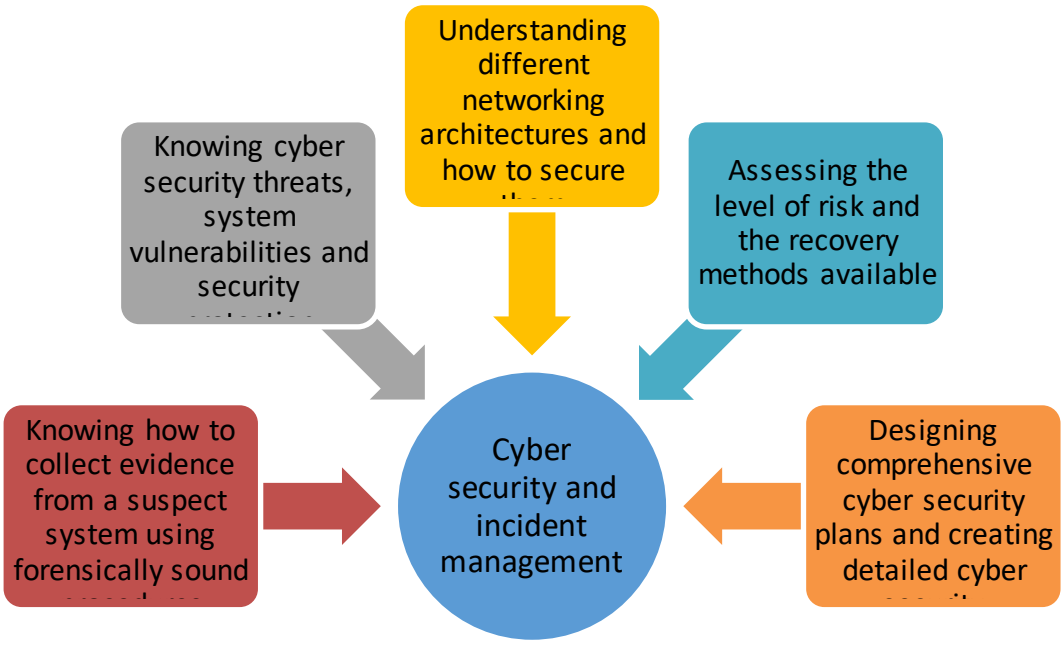
Unit 11: Cyber Security and Incident Management

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 mandatory externally assessed 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, correctly investigate and manage potentially devastating security incidents.

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



This unit provides learners with a sound foundation in security and computer forensic disciplines for higher education.

It would be ideal if the class or course had a virtual learning environment, as 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, the majority of the unit should be taught in an active fashion using targeted practical activities, particularly with regard to security and network-related concepts; therefore, this guidance recommends the use of pre-prepared disk images which contain the necessary resources or system 'snapshot', which will 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 and repositories are highly recommended.

Having quarantined network facilities and open source software available helps learners to simulate, detect, investigate and manage many different types of cyber security threats in a safe environment while providing a parallel to 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, making it possible to collect and use examples as real-world case studies. This helps to ground and contextualise many of the concepts that the learners are studying, often making quite technically austere material come alive in exciting ways.

Content area A: Cyber security threats, system vulnerabilities and security protection methods

This content area requires learners to demonstrate knowledge and understanding of technical language, security threats, system vulnerabilities, legal implications and security protection methods.

The investigation of different cyber security threats may be taught by exploring each type of threat and linking it to a real-world instance where the personal, financial, operational, reputational, legal or criminal impacts are very clear for the learner to see; this tends to reinforce the severity of each threat in learners' minds. Various approaches can be taken to help learners understand how external threats function, for example, there are many online videos which illustrate in a lively way how malware (malicious software) works or how to successfully hack a website or employ social-engineering techniques. Other possibilities include asking socially active ethical hackers or system administrators if they would be willing to act as guest speakers.

System vulnerabilities are best tackled by exploring each category (network, organisational, software, operating system, etc.) and selecting particular exploits that can be replicated, in particular replicated by each learner. 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 or accessing administrative web interfaces on Internet of Things (IoT) devices such as webcams via default passwords. Learners can also be encouraged to explore up-to-date sources of information for known hardware and software vulnerabilities to exploit, though this would require suitable supervision. More traditional forms of vulnerability, i.e. theft of portable hardware, can be best demonstrated by leveraging appropriate physical security measures designed to prevent this, such as security locks, CCTV and protected cabling.

The specific UK legislation thematically linked to this unit may be covered elsewhere, but traditionally, it is best taught through research and presentation.

Other techniques such as court-based role play using case studies may offer a viable and more active approach.

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. Once again, this is best delivered by means of demonstration and a round robin of practical activities which learners can try individually, in pairs or 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, and hardening server-side scripts to filter SQL injections. This technique allows learners to associate each potential threat with a practical solution; this preparation will be beneficial for Part A of their externally set task.

Content area B: Use of networking architectures and principles for security

This content area 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 that are used and the typical resources and services that the network provides.

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

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

Explore network infrastructure and services by pairing presentation and demonstration, supplemented by online videos and animations that detail their working (see Resources section). Clearly, the use of a quarantine network would enable learners to set up a DNS server, configure a DHCP service and populate typical directory services (DS) in a very active way. It may seem obvious, but not only is it rewarding for the learner to both configure the DHCP address pool on a server and change a networked client to obtaining its IP address from a dynamic DCHP request rather than using a static address, but it also makes the process exceptionally transparent and easy to understand. Try to demystify many such services and resources this way, including shared services (files and printers), web hosting and internal email. Again, where practical limits are felt in the classroom, many network visualisation tools, such as the Cisco Network Simulator, support simulated services, offering you a viable alternative – although there are open source simulators available, such as Cloonix and Mininet.

It should be noted 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 to network infrastructure and services, e.g. when demonstrating or configuring DHCP on a wireless network, stress that the assignment of an IP address could be reliant on the client device's MAC address being successfully filtered. This helps the learner to forge links between the two topics and is great preparation for Part A of the externally set task, which requires practical security solutions.

Content area C: Cyber security protection plan

This content area requires learners to assess risk vulnerabilities and the levels of risk attached to those vulnerabilities, evaluate protection methods and develop security plans which make reasoned judgements and draw conclusions about their efficacy.

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

In order to assess a computer system's vulnerabilities, it is vital that learners have access to quarantined systems that they can interrogate as well as a range of software tools for which they need to be given 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. Where possible, command-line tools should be preferred, as this will reinforce learners' reliance on Microsoft Windows and GUI-based utilities. The Open Web Application Security Project (OWASP) Top 10 (currently being collated for 2016) provides a good reference list of popular exploits of which learners should be made aware, perhaps studying some of these as selected case studies.

The perennial popularity of web application vulnerabilities (particularly poorly-written PHP, among others) suggests that the use of deliberately vulnerable applications makes an instructive test bed for learners to explore the impact and risks of poor programming. This type of activity can be particularly illustrative as it is possible for learners to exploit the application 'as is' from a web client, then amend the application's source code on the server using OWASP recommendations and finally try to exploit (usually unsuccessfully) from the client once more. Performing these 'real world' vulnerability fixes is good preparation for the type of thinking required when creating a cyber security protection plan.

For any identified threat, it is necessary for learners to calculate its risk severity using the recommended matrix (see unit content), which balances threat probability with impact level/value of the loss incurred. The best way to cover this process is to work through a set of threats and let learners decide, by applying the risk severity matrix, how urgently an appropriate protection measure show be selected and applied. Moderated group discussion, perhaps collating findings from smaller working parties, each with their own identified threat to rate, is often a good technique to employ here.

Asking learners to produce a cyber security plan for a system without first having seen a model paper is difficult. As such, although it is possible to present a checklist of content that would be expected in such a plan, e.g. software and hardware protection measures, risk assessment, constraints, legal responsibilities, etc., it is far more revealing to lead the reverse-engineering of 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) and realistically expect them to include similar content in the anticipated format.

Content area D: Cyber security documentation

This penultimate content area requires learners to be able to 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 270001:2013, typical organisation policies and policies that enforce relevant legislation, e.g. the Data Protection Act (DPA).

Governance policies, international standards and organisation-level policies can feel very remote if they are not grounded within the learners' everyday experience of IT systems and processes. Linking IT policies to the required complexity of their user passwords is perhaps one way to forge a connection. Backup of learner data and acceptable use of email and the internet may also provide easy rationales for IT policies. The challenge here is to ask learners to metaphorically 'cross the floor', thinking more like a technician trying to secure a system than an actual user who may resent the limitations the policies place on their user experience.

In addition, various forms of relevant legislation appear in many other units on the programme, so integration across subjects, e.g. data protection themes, is an entirely viable learning tactic.

Other areas of focus should include incident response and disaster recovery policy. 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, you will need to 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 that they establish with their clients. Moderating a prepared question-and-answer session on these agreements should identify any gaps in coverage that need to be addressed, e.g. particularly with regard to dispute resolution, etc.

Content area E: Forensic procedures

This final content area requires learners to analyse forensic evidence data and information to identify security breaches and manage security incidents.

Forensic computing principles rely on process and strict recordkeeping, particularly with regard to keeping a chain of evidence. As such, the key to delivering this part of the unit's content is to focus on the professional characteristics that this type of task demands – thoughtfulness, diligence and good organisation.

Use a popular Linux distribution to teach a number of new practical skills, e.g. cloning a file system, checking recently mounted devices, showing recent firewall activity, viewing configuration files and 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 several reputable websites that enable these types of activity. Guest speakers, perhaps from the institution's own network infrastructure and services team, may be willing to provide additional insight.

At every stage, it should be made clear to learners 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, conducted with model procedures, is perhaps the best way to deliver this content area, allowing learners to investigate a realistic scenario and gather their 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 in order 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. Removing existing protections or the deliberate creation of 'flawed' security settings are also obvious 'clues' that can be engineered.

Learners should initially be equipped with a good range of tools and techniques that make it possible to investigate, find and – most importantly – record the evidence they need without damaging or changing it. Note that learners will be required to complete a forensic incident analysis based on unseen evidence as part of their external assessment. Appropriate recording tools (electronic or paper-based) should be made available, along with examples of similar cyber security documentation (policies and procedures) that they can use to recommend revised security protection measures based on the evaluation of their forensic findings.

Assessment guidance

As an externally assessed unit, Pearson will provide a set task which must be completed under supervised conditions, contributing to 42% of the total qualification guided learning hours (GLH).

Learners are expected to complete this set task over a period of nine hours, split over a number of sessions occurring in a three-week period timetabled by Pearson. The task has two separate parts – Part A, taking five hours, and Part B, using the remaining four hours of the allotted time.

Both tasks should be completed in strict order using a computer and submitted electronically. There are 80 marks allocated for this task and it will be marked using a level-based mark scheme that is located in the programme's online Sample Assessment Materials.

Pearson will provide sample materials that you may use to help learners prepare for assessment. The availability of the task is December/January and May/June each year. The first assessment availability is May/June 2018.

Across Parts A and B, students will be expected to complete the following activities based on a realistic scenario:

- Risk assessment of the networked system
- Develop a cyber security plan for the networked system
- Write a management report with a solution justification – PDF document
- Prepare a forensic incident analysis based on realistic evidence (unseen)
- Write a management report detailing improvements in a given system.

See the SAMs for full details.

You can help to fully prepare learners by creating micro-tasks which duplicate elements of the task provided through Pearson's sample materials, working through these with learners in an interactive and mentoring fashion. Draw out learners' technical understanding, assumptions and exactly how they are

interpreting the task; many marks are often lost due to misinterpretation and misunderstanding.

Students planning will need to include the following information:

1) Threat(s) addressed by the protection measure
2) Details of action(s) to be taken
3) Reasons for the actions
4) Overview of constraints – technical and financial
5) Overview of legal responsibilities
6) Overview of usability of the system
7) Outline cost-benefit

Analysis of the sample mark scheme will help learners to discover the level of thought processes, problem-solving and scope that their answers must provide at this level, making the division between pass and distinction grade descriptors much more transparent.

Above all, advise learners that the appropriate use of technical language needs to be consistently high throughout both parts of the set task to achieve higher grades.

Getting started

This provides you with 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 the learners' experience with security issues and vulnerabilities; many may have experienced having their access to products and services denied due to system outages caused by cyberattacks or internal failures. The tutor can reference current events such as recent high-profile attacks (2016) including Tesco Bank, Talk Talk or Sony PlayStation.

A secondary thread to follow that cements the importance of the unit is to ask how many day-to-day activities involve the use of computers, particularly those that store, process and communicate valuable, private or critical data. Combining this with tell-tale statistics such as the excessive number of probes and hacking attempts a typical website receives each day will hopefully reveal the scale of the problem that IT security professionals face.

Where possible, most aspects of this unit should be taught in a practical manner; although there is certainly a considerable amount of theoretical knowledge for the 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 being able to select and use the necessary tools and techniques appropriately.

You may also consider appointing (or asking for volunteer) learners with more networking or operating system experience, particularly with Linux distributions, to act as classroom support.

Content area A / Topic A1 – Cyber security threats

You will detail different types of cyber security threats.

- Differentiate between internal and external threats.
- Lead a presentation, complete with sample case studies and examples, that shows how internal threats occur, e.g. sabotage, theft, natural disasters (flood, etc.), unauthorised access, system vulnerabilities and unsafe practices, etc.
- Lead a presentation, complete with sample case studies and examples, that shows how external threats occur, e.g. malicious software (different types), hacking (individual, commercial and government sponsored), sabotage and social engineering.
- Follow up with 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 for identification in risk assessments.
- Ask learners to cloudburst how organisations can keep abreast of the changing landscape of cyber security threats and protect their operations and data.
- A template for the cyber security plan can be found on the Pearson website – it is highly recommended that this is used as it ensures complete coverage of the requirements.

Content area A / Topic A2 – System vulnerabilities

You will detail different types of system vulnerabilities.

- Lead a presentation, with supporting practical demonstrations, of different types of system vulnerabilities, for example, a badly configured firewall, poorly selected file permissions or user privileges, weak password policy, etc.
- Demonstrate the dangers posed by software applications. This could be achieved by downloading an infected application from an untrusted source onto a quarantined PC and observing the impact, performing an SQL injection attack on an insecure web application, etc.
- Discuss topical references, 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. CVE database. Note: it may be practical to duplicate well-chosen examples in a controlled network environment.
- Ask learners to create informational posters which demonstrate common attack vectors, including Wi-Fi, Bluetooth, etc.

Content area A / Topic A3 – Legal responsibilities

You will detail the relevant UK and EU (European Union) legislation that applies to different systems.

- Ask learners to summarise relevant UK and EU legislation, presenting their findings to their peers. A blog, wiki or podcast could be suitable vehicles.
- Lead a discussion that links the different legislation available to how an organisation (and individuals) should respond.
- Compare and contrast with similar legislation available internationally, e.g. 2001 USA Patriot Act, 1998 Digital Millennium Copyright Act (DMCA), etc.
- Explore news stories and case studies that incorporate prosecutions under UK and EU legislation. Encourage learners to consider the impact of internet-based cybercrime on the sovereignty of legal authority.

Content area A / Topic A4 – Physical security measures

You will 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 the physical security measures used to secure specific locations such as hosting companies and data warehouses. Opportunities may exist to send small parties of learners on industrial visits to this type of location by arrangement.
- Demonstrate use of biometric devices to access systems, e.g. unlocking a desktop PC using a fingerprint scanner.
- Discuss physical security measures as applied to data storage, data protection and backup procedures.

Content area A / Topic A5 – Software and hardware security measures

You will explore various software and hardware security measures with learners.

- Lead, demonstrate and support round-robin practical activities which:
  - task learners with installing various types of anti-virus software, updating their signatures and selecting appropriate actions to disinfect affected files.
  - task learners with installing and configuring 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.
  - task learners with testing 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).
    - allow learners to 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. Make sure each commercial example has 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.

Content area B / Topic B1 – Network types

You will introduce the concept of different network types, their topologies, components, services and resources.

- Present the applications and features of networks. Networks can be introduced in ascending order (e.g. PAN to WAN) and terms like intranet, extranet, internet and cloud should be fully defined and differentiated.
- Discuss physical and logical topologies and ask learners to explore different types; asking learners to create network topology posters can be instructive as they are visual in nature.
- Using appropriate media, connections and devices, 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 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.

Content area B / Topic B2 – Network components

You will 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. Activities for learners could include:
    - 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.

Content area B / Topic B3 – Networking infrastructure services and resources

You will 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 are able to use such tools to track packets 'in' and 'out' of their computer, inspecting the data being sent and 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, Dynamic Host Configuration Protocol (DHCP), routing and 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. A good example is to enable a web server on a quarantine LAN and access its resources via a client using HTTP requests. The whole HTTP request and response process can be tracked 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. Demonstrate real-time modifications to the served content by requesting the resource again.

Content area C / Topic 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 being the probability of the threat occurring multiplied by the expected impact level/value of the loss.
- Differentiate risks as being 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 being unlikely, likely and very likely.
- Differentiate the impact level/value of the loss as being minor, moderate or major.
- Ask learners to create a risk severity matrix (opportunities exist here for manual diagrams, word-processed tables, spreadsheets, website forms or programmed solutions).
- Using a given set of real-world scenarios, ask learners to assess the probability and impact levels and thus calculate the risk severity. Discuss findings with learners.
- Review risk assessment approach and methods.

Content area C / Topic 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.
- After separating learners into groups of three or four, ask them to construct a document for a selected case study (after they have investigated, identified the vulnerabilities and assessed their risks) with realistic expectations of them including similar content in the anticipated format. Note that learners will need to cover the following areas in their assessment:
  1) Threat(s) addressed by the protection measure
  2) Details of action(s) to be taken
  3) Reasons for the actions
  4) Overview of constraints – technical and financial
  5) Overview of legal responsibilities
  6) Overview of usability of the system
  7) Outline cost-benefit
- Ask learner groups to swap their plans with their peers and task them with evaluating whether the protection measures would work as intended, identifying any good practice and possible areas for improvement.

Content area D / Topic D1 – 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.
- Discuss and explore incident response policy.
- Discuss and explore disaster response policy.

Content area D / Topic D2 – External service providers

Explore the role of an External Service Provider (ESP).

- Discuss ESP agreements for cloud services, applications and storage.
- Discuss ESP agreements for hardware and software.
- Present the implications of ESP agreements.
- Ask learners to determine which types of agreements may be covered by data protection laws.

Content area E / Topic E1 – Forensic collection of evidence

Detail the process of collecting evidence using a forensically sound methodology after a security incident.

- Present desktop forensic activities.
- Lead and support practical sessions that impart new 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 with learners.
- Examine the procedures required to perform network forensics.

Content area E / Topic E2 – 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 attain them.
- 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) and ascertain whether or not a single cause can be clearly proven.
- Ask learners to make recommendations on how to prevent similar security incidents from reoccurring in the future in the form of a report. Learners should draw on security measures that they have already been taught, but they must justify their selections appropriately.
- Provide learners with feedback on their recommendations.

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

- Unit 1: Information Technology Systems
- Unit 2: Creating Systems to Manage Information
- Unit 3: Using Social Media in Business
- Unit 4: Programming
- Unit 6: Website Development
- Unit 7: Mobile Apps Development
- Unit 8: Computer Games Development
- Unit 9: IT Project Management
- Unit 12: IT Technical Support and Management
- Unit 13: Software Testing
- Unit 14: IT Service Delivery
- Unit 15: Customising and Integrating Applications
- Unit 16: Cloud Storage and Collaboration Tools
- Unit 19: The Internet of Things
- Unit 21: Business Process Modelling Tools

Further/complimentary study could include:

Vendor-specific qualifications, e.g.

Cisco Entry and Cisco Associate

http://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html

Vendor-neutral qualifications, e.g.

CompTIA Network+

https://certification.comptia.org/certifications/network

CompTIA Security+

https://certification.comptia.org/certifications/security

Resources

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

Textbooks

- Clarke, Justin, 2012, *SQL Injection Attacks and Defense*. Elsevier. ISBN-10: 1597499633, ISBN-13: 978-1597499637

  Understanding SQL injection, one of the most well-known security vulnerabilities on the internet.

- Clark, Ben, 2013, *Rtfm: Red Team Field Manual.* CreateSpace Independent Publishing Platform; ISBN-10: 1494295504 ISBN-13: 978-1494295509

  RTFM contains the basic syntax for commonly used Linux and Windows command line tools.

- Lowe, Doug, 2016, *Networking All-In-One For Dummies*. John Wiley & Sons, sixth revised edition; ISBN-10: 1119154723, ISBN-13: 978-1119154723

  Details network planning, administration, protocol, virtualisation, cloud networking, servers, etc.

- Mandia, Kevin et el, 2014, *Incident Response & Computer Forensics*. McGraw-Hill Education, third edition. ISBN-10: 0071798684, ISBN-13: 978-0071798686

  Covers the entire lifecycle of incident response, including preparation, data collection, data analysis and remediation.

- Meeuwisse, Raef, 2015, *Cybersecurity for Beginners*. Lulu Publishing Services, ISBN-10: 1483431231, ISBN-13: 978-1483431239

  Overview and discussion on the essentials of cybersecurity, including a number of case studies and a good glossary of terms.

- Nikkel, Bruce, 2016, *Practical Forensic Imaging: Securing Digital Evidence with Linux Tools.* No Starch Press, ISBN-10: 1593277938, ISBN-13: 978-1593277932

  A text that shows how to secure and manage digital evidence using Linux-based command line tools, many of which are open source.

- Sammons, John, 2015, *The Basics of Digital Forensics*. Elsevier, second edition, ISBN-10: 0128016353, ISBN-13: 978-0128016350

  An introduction to computer forensics, covering a range of devices, key concepts and the tools needed to perform examinations. This text also includes guidance on how to collect evidence, document the scene and recover deleted data.

Journals

- Cyber Defense Magazine

  http://www.cyberdefensemagazine.com/magazine/

  A magazine dedicated to IT security

- Digital Forensics Magazine

  https://digitalforensicsmagazine.com/

A magazine that investigates the digital world

- SC Magazine UK

  https://www.scmagazineuk.com/

  A cyber security magazine with cyber-crime and business news

Videos

- Hack All The Things: 20 Devices in 45 Minutes

  https://www.youtube.com/watch?v=h5PRvBpLuJs

  A lecture revealing 20 device vulnerabilities and how they can be exploited.
- SQL Injection Basics Demonstration

  https://www.youtube.com/watch?v=h-9rHTLHJTY

  A demonstration of using SQL injection techniques to exploit a web application.
- Vulnerability Assessment and Mitigating Attacks

  https://www.youtube.com/watch?v=tiCCi8pX270

  A simple overview of these concepts.
- Computer Forensic Tutorials

  https://www.youtube.com/playlist?list=PL6oHuo5it4TgA-ZtIo3x5G0l0HDwPPZ9d

  A series of computer forensic tutorials from O'Reilly with videos that cover capturing traffic, volatile information, checkpoints, Unix tools, forensic toolkits, etc.
- Network Threats: Port Scanning

  https://www.youtube.com/watch?v=N5sKVaQLYjY

  Part of a larger series on network threats, this instalment focuses on port scanning (for both validation of security policy and vulnerability reconnaissance).
- NETWORK TYPES: LAN, WAN, MAN, WLAN, PAN, SAN

  https://www.youtube.com/watch?v=7RBddlGeyqY
- A complete overview of the different types of network. Automatic IP Address Assignment: How DHCP Works

  https://www.youtube.com/watch?v=RUZohsAxPxQ

  Explains the concept of DHCP, an application-layer protocol that your own computer probably uses to get an IP address from your network.

Websites

- Acunetix Vulnerability Scanner

  http://www.acunetix.com/vulnerability-scanner/

  Automated tool which crawls a website looking for common vulnerabilities.
- Cisco Packet Tracer

  https://www.netacad.com/about-networking-academy/packet-tracer/

  Free network simulation and visualisation tool.
- Cloonix

  http://clownix.net

Open access network simulator

- Common Vulnerabilities and Exposures (CVE)

  https://cve.mitre.org

  An online dictionary of common names for publicly known information security vulnerabilities.

- Mininet

  http://www.mininet.org

  Open Source Network Simulator

- The National Vulnerability Database (NVD)

  https://nvd.nist.gov/

  The NVD is updated whenever a new vulnerability is added to the CVE dictionary of vulnerabilities. The vulnerabilities are then analysed by NVD analysts and augmented with vulnerability attributes.

- Forensic Control

  https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

  Introduction to computer forensics

- How Domain Name Servers Work

  http://computer.howstuffworks.com/dns.htm

  Overview of DNS by howstuffworks.com.

- OpenLDAP

  http://www.openldap.org/

  OpenLDAP Software is an open source implementation of the Lightweight Directory Access Protocol.

- Open Web Application Security Project (OWASP)

  https://www.owasp.org/index.php/Main_Page

  Worldwide not-for-profit charitable organisation focused on improving the security of software.

- Penetration testing practice lab – vulnerable apps / systems

  https://www.amanhardikar.com/mindmaps/Practice.html

  A portal of links to vulnerable web applications, operating system installations, etc.

- Wireshark

  https://www.wireshark.org/

  Wireshark is, according to its publisher, the world's foremost and most widely used network protocol analyser.

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 students to access them through the school/college intranet.