Unit 3 – Cyber Security

Unit Overview:

The need for secure digital systems is more crucial than ever before. We rely on computerised systems and networks to collect, process, store and transfer vast amounts of data and to control critical systems such as water and power supplies. Business and e-commerce can be undertaken twenty-four hours a day, seven days a week and telecommunications enable us to keep in touch with family and friends and collaborate with colleagues at any time. Mobile devices offer us freedom and flexibility of where and how we learn and work. However, for all the advantages that these systems offer us, some people have found ways to exploit them and this poses a threat to our safety and security in the real world, as much as in the cyber world.

To deal with this problem the cyber security industry is expanding at a rapid rate. This unit has been designed to enable you to gain knowledge and understanding of the range of threats, vulnerabilities and risks that impact on both individuals and organisations. You will learn about the solutions that can be used to prevent or deal with cyber security incidents resulting from these challenges. You will be able to apply your knowledge and understanding of cyber security issues and solutions by reviewing and making recommendations for ways to best protect digital systems and information. The unit also makes reference to UK government cyber security initiatives, for example, the UK government's The UK Cyber Security Strategy, Cyber Essentials Scheme, 10 Steps Strategy and Cyber Streetwise.

Learning Outcomes:

- **LO1:** Understand what is meant by cyber security
- **LO2:** Understand the issues surrounding cyber security
- **LO3:** Understand the measures used to protect against cyber security incidents
- **LO4:** Understand how to manage cyber security incidents

Assessment:

- Assessment is a 1hr formal external assessment taken under exam conditions.
- The duration is 60 Minutes
- The paper is worth 60 Marks
- Section A is based on Pre-release materials delivered 30 Days prior to the exam and is worth 42 Marks, 70% of the total awarded.
- Section B will contain unassessed content from Section A and is worth 18 Marks, 30% of the marks awarded.

There is a strong emphasis on retention and application to the key vocabulary and demonstration of wider, real life knowledge and this should be the core focus for the delivery of this unit.

<table>
<tr><th>Lesson:</th><th>Lesson Outcomes:</th><th>Suggested teaching:</th><th>Key Terms</th></tr>
<tr><td>1.1. Cyber security aims to protect information

1 Lesson</td><td>TBAT:
Understand the need for cyber security and the essential role it has in maintaining a functional society.</td><td colspan="2">Do Now: Students to create a mind map to reflect on all the technology that they use on a daily basis.

This should involve subscription services, social media, educational platforms and external agencies such as school and health officials and the impact of down time.

Layering on the mind map students should reflect on the terms Personal, Sensitive and Financial data.

Students should define the 3 key terms and provide examples from their mind maps in the definitions of confidentiality, integrity availability.</td><td>• Confidentiality
• Integrity
• Availability</td></tr>
<tr><td rowspan="2">1.2 Types of cyber security incidents

2 lessons</td><td rowspan="2">TBAT:
To link the key categories of data threats to the main types of attackers.</td><td colspan="2">Do Now: Introduce students to the different threats/types of incidents that can occur.

Students could be tasked to research the following types of cyber security incidents and provide details of at least one example of each type of incident that they research linking them to the types of attackers.

To help students organise their thoughts and responses this could be done in a tabular format.</td><td rowspan="2">As listed</td></tr>
<tr><td>Types of Threats:
• Unauthorised access
• Disclosure
• Modification
• Inaccessible
• Destruction
• Theft</td><td>Types of Attackers:
• Hacking
• Disclosure of government information Impairing the operation of a digital system Denial of service
• Malware
• Identity theft</td></tr>
<tr><td>1.3 The importance of cyber security

1 lesson</td><td>TBAT:
To be able to articulate the impact of cyber security and</td><td colspan="2">Do Now: Teaching should focus on the different types of data that need to be kept secure: personal data, an organisation’s data and a state or country’s data.

Students could work in pairs or small groups and list as many types of personal data, organisational data and national data as possible, building on LO1.</td><td>• Protection of Personal data
• Organisational data</td></tr>
</table>

<table>
<tr><td></td><td>the needs for stringent levels of protection.</td><td colspan="2">They could then consider cases in which data has been compromised:

https://www.youtube.com/watch?v=0p3787JiFgQ
A short video (8 minutes) by VM news, ‘10 Cyber Security Facts’.

Assessment:
Learning Outcome Reflection, a range of questions reflecting on delivered LO1 content this should incorporate 2, 2 Mark questions and 1 extended response (6 Marks) based on the importance of cyber security.</td><td>• State data</td></tr>
<tr><td rowspan="2">2.1 Threats to cyber security

1 Lesson</td><td rowspan="2">TBAT:
Define the terms vulnerabilities and explain potential threats to their personal data.</td><td colspan="2">Do Now: Teaching should begin by introducing the term vulnerability and check that learners understand its meaning. This could be done through an activity such as 4 pics 1 word.

Students could be tasked with assessing the software, hardware, network and people vulnerabilities of the systems that they use in school/college/work/home. Students could refer to the following resource:
A video (39 minutes) on Security Concepts: Computer Security Lectures 2014/15 S2, An overview of cyber security issues (Leeds Beckett University)
https://www.youtube.com/watch?v=pLEVNl8KtO4&list=PLUhmDd3hiISlAbnD8eWlDjetsj1eJmiZs

A video (5 minutes) on Social Engineering –
https://www.youtube.com/watch?v=xcJV2JGeVn0

They could present their findings in the form of a report or an information leaflet.</td><td rowspan="2">As listed</td></tr>
<tr><td>Vulnerabilities:
- System attacks
- Physical threats
- Environmental</td><td>Threats:
- Accidental
- Intentional
- Organised Crime
- State sponsored</td></tr>
</table>

2.2 Types of attackers **2 lessons**	**TBAT:** Discuss the social and political context of state sponsored attacks with USA and Russia.	**State Sponsored Attacks:** **Do Now - Reading Activity:** Students should begin by reflecting on the historical context of the Cold War. This should be discussed with the group to ascertain their levels of knowledge of the current political landscape between these countries. Students Should now read a news report from the Guardian depicting the relationship in December 2020. https://www.theguardian.com/world/2020/dec/18/cyber-attack-brutal-reminder-russia-problem-facing-joe-biden Students should reflect on the article evaluating the relationship at that point. Students should summarise the Who, What and Why. Collectively review the following interviews given by Joe Biden the president elect, and Vladimir Putin following a summit in March following the G7 summit that Russia is no longer a part of. https://www.youtube.com/watch?v=1MciD4ciyNk https://www.youtube.com/watch?v=LpFHfywKzLY Students to complete the following topic summary page: LO2.1 - State Sponsored Attacks - Topic Summary Page.pptx	• Cold War • Infrastructure • G7 • Summit • President elect • Voting • Political Advantage
2.2 Types of attackers **1 lesson**	**TBAT:** Describe the moral dilemma of Hacktivists and explain how they perceive their actions are for	**Do Now:** Students watch the trailer for Mr. Robot (15) This is a popular dramatization that reflects on many of the key concepts of the current learning outcome. (Outsider, Hacktivist, Greater Good and moral dilemmas) Students must record five keywords that spring to mind when watching the trailer. – Possible use of online wordle. https://www.mentimeter.com/features/word-cloud	• Moral • Ethical • Greater Good • Dilemma

	the greater good.	Students must define the term hacktivist and research and review a chosen example. This should be a reflection on both sides of the story including the Hacktivist (perpetrator) and the victim. **Assessment:** A hacktivist is a threat to cyber security. Explain the characteristics of a hacktivist and who they may target. (6)	
2.2 Types of attackers **1 lesson**	**TBAT:** To define the term Bot Net and create an implementation diagram of an attack.	**Do Now:** Students begin by viewing an overview report of a botnet attack. **Botnet:** https://www.youtube.com/watch?v=3BbxUCOFX8g Students should review the video and create a Bot Net attack implementation diagram. **Denial of Service:** Additional supplementary video on the Denial of service attacks is here https://www.youtube.com/watch?v=yLbC7G71IyE **Assessment:** Please define the term Botnet and explain how the process undertaken to instigate a cyber-attack using this method. (6)	• Bot Master • Zombie • Dormant • Trojan • Host server
2.2 Types of attackers **2 lessons**	**TBAT:** Define the term Malware and understand the primary malware types.	**Do Now:** Students must define the term Malware, understanding the etymology, Malicious and Software. 3 students are provided with Key Questions and videos that they must independently review and record answers for the following types of Malware. **Zero Day:** https://www.youtube.com/watch?v=xZc6mD9PSI4 **Stux Net:** https://www.youtube.com/watch?v=7g0pi4J8auQ	

		Heartbleed: https://www.youtube.com/watch?v=6Sz5wBBXzpc **SQL Injections:** https://www.youtube.com/watch?v=FwIUkAwKzG8 Staff should conclude the lesson by having a group reflection on responses identifying any common misconceptions.	
2.2 Types of attackers **1 Lesson**	**TBAT:** Define the different categories of Hackers and Vulnerability Brokers.	**Do Now:** In the starter activity students should review the connotations of colour. Light positive – dark negative. Introduce the content of black hack hackers as those who are negative and in it for personal gain. Introduce the theory of white hat hackers and the notion supporting other. Students should also review Vulnerability Brokers and how they use their expertise to exploit individuals and organisations. The outcomes from this could be collate in a short report or revision guide. **Assessment:** Define three types of attackers and explain their motivations for exploiting vulnerabilities. (9)	

<table>
<tr>
<td>2.3 Motivation for attackers

1 Lesson</td>
<td>TBAT:
To summarise knowledge of all types of attackers and their motivations.</td>
<td>Do Now: Students should start by identify the icons for the types of attacks. Insider previously not covered so will require discussion – Link to Mr Robot video previously watched.

Student to complete a table that:
• Defines Attackers
• Discusses typical characteristics
• Describes motivations for attacks

 
</td>
<td></td>
</tr>
<tr>
<td>2.4 Targets for cyber security threats</td>
<td colspan="3">This learning outcome will not be taught as a discrete lesson, rather it is to be interleaved with other content throughout the unit.

Content to be covered:

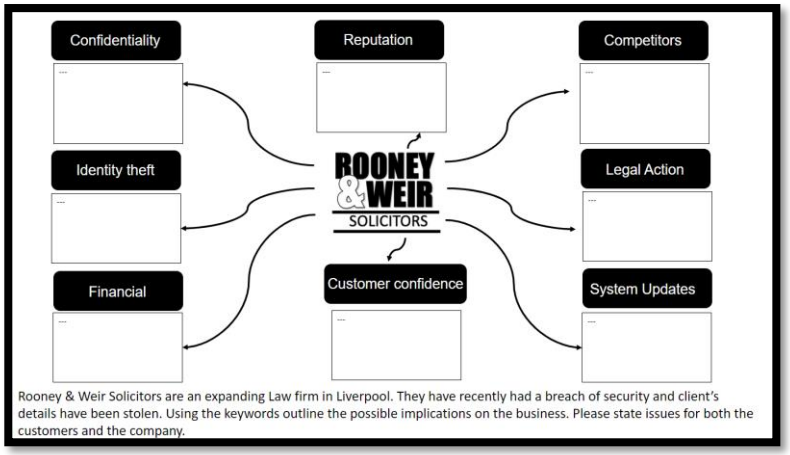
People - organisations - equipment – information</td>
</tr>
<tr>
<td>2.5 Impacts of cyber security incidents

1 Lesson</td>
<td>TBAT:
Describe the impact of cyber attacks on a company and their clients.</td>
<td>Do Now: Students to review a case study of a local solicitors and look at the impact of such an attack on the solicitors and their clients.

Key vocabulary to be reviewed:

Loss: Confidentiality, integrity, availability, data, finance, business, identity, reputation, customer confidence

Disruption: including people's lives, business, industry, transport, industry, the media, utilities

 
</td>
<td>• DDOS
• Botnet
• DNS
• Internet Traffic
• Redirected
• Collapse
• Services
• Impact
• Outage
• Duration
• Communication
• Healthcare
• Security
• Entertainment</td>
</tr>
</table>

		Safety: including identity theft, oil installations, traffic control Students to complete the attached mind map document. **Case Study review:** Students to review the following case study and summarise in 2 paragraphs incorporating all the key vocabulary. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet	
2.6: Other considerations of cyber security **2 lessons**	**TBAT:** Understand the legal implications of cyber-attacks.	**Do Now:** Students begin by listing 8 principles of the Data Protection Act from memory. Student must review the following 4 governing legislative acts that determine how we access, control and distribute information. • Regulation of investigatory Powers Act 2000 • The Computer Misuse Act 2000 • The Data Protection Act 1998 • General Data Protection Regulation (GDPR) Students must create a guide for Rooney & Weir Solicitors that summarises the content and makes and operational guide for the usage, storage and distribution of data. **Assessment:** Learning Outcome Reflection, a range of questions reflecting on delivered LO2 content this should incorporate 2, 2 Mark questions and 1 extended response (6 Marks) based on the threats and impact of a cyber security attack.	• Ethical • Legal • Operational Implications for stakeholders

3.1 Cyber security risk management **2 lessons**	**TBAT:** To describe methods of testing as a means of mitigating risks to data	**Do Now:** Students will be given 3 icons/images and they must describe what they believe they represent and how they are used to protect data. This is the first of 2 lessons that look at how we mitigate risks by: - Testing for potential vulnerabilities - Monitoring and controlling systems - Protect vulnerabilities  **Vulnerability Testing:** https://www.youtube.com/watch?v=4gYYVghLVEY Students to review the video and record notes on the similarities and differences in Penetration Testing and Vulnerability Testing. **Fuzz Testing:** https://www.youtube.com/watch?v=iIWpIL66DLE Students to record notes on fuzz testing and how it is used to discover vulnerabilities in a system. **Sand Boxing:** https://www.youtube.com/watch?v=29e0CtgXZSI Students to review the video and record notes on Sand Boxing. Students must state that this is an artificial environment that is self-contained and allows for the use of viral infections that will pose no threat to the wider system.	Self-contained Environment Overload
3.1 Cyber security risk management **3.2 Testing and monitoring measures**	**TBAT:** To define intrusion detection and prevention systems and know which is the most	**Do Now:** Is prevention better than cure? What is the link with intrusion detection and intrusion prevention? Students must understand the key terms: • IPS • IDS • HIDs	• Intrusion • Detection • Prevention • Monitor • Control • Network Based • Host Based

1 Lesson	effective in protecting data.	• NIDs Task 1: Key Word Dissection Students record definitions for all keywords. Task 2: System Definitions: Watch the videos and complete the notes detailing the functionality of both systems. A. https://www.youtube.com/watch?v=_gHMkEKGwBM B. https://www.youtube.com/watch?v=rvKQtRklwQ4 Task 3: Diagrams By remembering the layout and structure graphically it will also help you remember how the systems operate. Research and find 2 simplified examples of the system architecture.	• Signature Detection • Heuristic Detection
3.3 Cyber security controls (access controls) **3 Lessons**	**TBAT:** To describe different measures to ensure data is secure	**Do Now:** Students to list as many ways as known to ensure safety of data on white boards. They should then be presented with the categories to ask them to arrange them. • **Physical:** biometric access, swipe cards, alarms • **Hardware:** including cable locks, safes • **Software:** including firewalls, anti-malware, operating system updates, patch management • **Data:** including in use, at rest, in-transit, in the cloud • **Encryption:** including disks, databases, files, removable media, mobile devices • **Procedures**: including access management, data backup, remote working, device management, user accounts and permissions, awareness and training Students should make a guide for a Local Primary School on how to keep their data safe. It should include information on all the categories listed with the following details: • Definitions	• Cryptography • Biometric • Biology • Measurement • Metric

		• How to set up • How it will protect the IT systems and the data it contains. Learning Outcome Reflection, a range of questions reflecting on delivered LO3 content this should incorporate 2, 2 Mark questions and 1 extended response (6 Marks) based on the how to manage risks and vulnerabilities.	
4.1 Responding to an incident **1 Lesson**	**TBAT:** To describe different measures to ensure data is secure	Do now: Students enter the room and are told that all systems are down and we have no access to their data/work. They must list the priorities and decide who is responsible to each task. David Allerton to support with real life examples. Students will review a cyber security incident in school they must complete the following analysis: • Know responsibilities – Who is responsible for what • Know who to contact – who are the key agencies or stakeholders we must contact • Know procedures – what are the operational procedures to be carried out • Know the extent of the incident – categorisation of the incident, how do we know the damage done? • Contain the incident – What steps can be undertaken to contain the incident? • Eradicate the incident - – What steps can be undertaken to eradicate the incident? Review a case of a virus. • Reduce the impact of the incident • Recover from the incident • Confirm the system is functioning normally	•
4.2 Cyber security incident report **1 Lesson**	**TBAT:** Complete a Cyber Security Incident Report.	**Do Now:** Students read and review 2 emails detailing a cyber security incident. Students will read the 2 emails detailing the communications between a Network manager and a staff member. Students should complete the Cyber security incident report template. LO4 - Incident Report.docx	• Critical • Significant • Minor • Negligible • Intended Purpose • Response • Future management

Pre-release Materials:

A pre-release scenario will be provided prior to the exam. This is unseen until published 6 weeks prior to the exam. Students should aim to spend 12 Hours completing this review.

This will provide a context to the exam section A – 70% of the paper. This must be reviewed in preparation for the exam. The pre-release contains:

- **An introduction:** This will detail the organisation and the industry they operate within. This will provide an insight into the nature of the questions in the exam.
- **Network diagram:** This will detail the ICT system set-up and functionality. This should also be reviewed for any vulnerabilities or weaknesses.
- **Key Staff:** A key staff member will be identified, normally a network manager or director of Cyber Security. This will outline their job role and responsibilities.
- **Further Research:** A range of key bullet points will be provided for additional research and development of revision. A number of specific questions will be based on this content. As this is provided the mark scheme is very robust on the usage of key terms and the application of knowledge specific to this scenario. Example further research is identified below:

  To prepare for the examination, you should research the following themes:•
  - The different types of data stored by Stevenson Research and their importance
  - Different types of cyber security threats that Stevenson Research may be subjected to
  - Different types of attacker, their characteristics and motivations for attacking Stevenson Research.
  - The impact of a cyber security incident on Stevenson Research.
  - Justification for the different methods of mitigating risk.
  - The use of different types of detection systems.

- Students will revisit content delivered in LO1, LO2, LO3 and LO4 and create a full set of revision notes in relation to the further research topics. These should be collated in a centralised file.

Walking talking Mocks:
In addition to this time should be allocated for a walking, talking mock to walk through a test paper with students so that they understand the format of the paper, assessment and application of the marks scheme. Timings are vital as it is a 60 Minute paper and there is a lot of content. Students frequently run out of time.

Walking Talking Mock - 1 - April 2021.pptx