KNOWLEDGE ORGANISER

Unit 3

Cyber Security

KEY TERMS

KNOWLEDGE ORGANISER

How to use this booklet

This booklet contains all of the KEY TERMS for unit 3—Cyber Security. It is vital that you learn each term. This will help you to understand the questions in the exam.

You will be informally tested on these terms once a week.

It has been proven that if you write something 3 times then you

Read The definition a couple of 

Cover The 

Remember The definition, think about it 

Write Write what you remember 

Repeat Each step until you can write the definition 

"Whatever you think about, that's what you remember. Memory is the residue of thought."

- Daniel Willingham

Signature based	A digital signature is code that is attached to an electronically transmitted document to verify its contents and
Social engineering	Hackers use this non-technical method to access computer systems/networks without authorisation. It involves fooling people into breaking normal security procedures, such as guarding their passwords and relies on manipulating the good nature of individuals.
Spyware	Malware software that is designed to obtain covert information about someone else's computer activities by transmitting data covertly, from their hard drive, for example key logging software.
Threat	An action that when performed on a computer system/network can cause destruction or disruption, for example, a hack or malware.
Unauthorised access	Gaining access into a computer system/network illegally.
Virus	Malicious software which is capable of copying itself and corrupting computer systems/networks or destroying data.
Vulnerability	Is a weakness in a computer system/network that can be exploited by a threat, for example, out of date anti- malware software can result in the threat of a malware attack. If a computer system/network's vulnerabilities can be found and dealt with, this will help to minimize threats and risks.
Vulnerability broker	An individual who exploits a vulnerability or weakness in a computer system/network for gain, for example, a hacker.

Mitigate	To lessen an impact, for example, the impact of a cyber security incident or a risk.
Patch management	Acquiring, testing and installing code changes or patches to software on a computer system/network.
Penetration testing	A software tool that tests a computer system/network to find vulnerabilities that could be exploited by an attacker.
Phisher	An individual that attempts to acquire personal information, often for malicious reasons, such as fraud, by pretending to be a known and trusted individual or organisation.
Phishing	The act of attempting to acquire personal information, often for malicious reasons, such as fraud, by pretending to be a known and trusted individual or organisation.
Non repudiation	Ensures that an individual cannot deny the authenticity of their signature on a document or the sending of a message that they sent.
Risk	A threat to a computer system/network can result in a risk, for example, if a hacker gains access to a person's computer, there is a risk that data will be stolen.
Risk analysis	This involves analysing a computer system or a set of procedures and assessing whether a system is at risk from a cyber-incident due to weaknesses or vulnerabilities in software, hardware or procedures.
Risk management	This refers to ensuring that risks are monitored carefully and mitigated against or eliminated from a computer system/network.
Sandboxing	This is a security method for separating running programs on a computer system/network. It is often used to run untested code, or untrusted programs from unknown sources such as suppliers, untrusted users and untrusted websites.
Scammer	An individual who attempts to gain, for example, money from another person by fraudulent means enabled by the use of computers and the Internet.
Script kiddie	An individual who uses existing computer scripts or codes to hack into computer systems. They do not have the expertise to write their own code.

Key term	Explanation
Access management	Managing the access to a computer system/network. It includes procedures such as account administration, account maintenance, account monitoring and the revocation of an account.
Account lockout	A software security method performed by operating system software that locks any account when a user fails a login attempt more than a set number of times. For example, system software can be set up to lock an account for several hours if the user fails the login three consecutive times in a set time frame.
Anti-malware	Software designed to prevent, detect and eradicate malicious software, such as a virus or a worm.
Anomaly based	Software that is designed to detect computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
Asset	Something that is of value to a person, an organisation or a state, e.g. data, finance and secrets that should be secured against cyber security incidents.
Attacker	Individuals or organisations that target computer systems/networks illegally.
Audit trail	A record of activities on a computer system/network, for example, a record of modifications to data or access to parts of a system/network.
Availability	Data/information stored on a computer system/network must be available to authorised users and organisations and be protected from unauthorised deletion.
Biometric access	Access to a computer system/network using technologies that measure and analyse human body characteristics for authentication purposes, such as DNA, fingerprints, retinas, voice patterns, facial patterns and hand measurements.
Botnet	A network of computers infected with malicious software and controlled without the owners' knowledge,

	for example, to send spam or hoax emails.
Business continuity plan	A plan to continue operations that an organisation will follow if it is affected by a cyber security incident
Confidentiality	Information stored on a computer system/network must be protected against unintended or unauthor- ised access. Data confidentiality is a measure of the ability of a system to protect its data.
Cyber criminal	An individual who commits illegal activities using computers and the Internet.

Key term	Explanation
Cyber dependant	Illegal activities dependent on the use of computers and the Internet, such as hacking or the distribution of malware on a network.
Cyber enabled	Illegal activities that could be undertaken without the use of computers, such as fraud but that are enabled by the use of computers, such as fraudulently obtaining money for goods online.
Cyber security	Refers to technologies, processes and practices designed to protect computers, networks, software and data from attack, damage or unauthorised access and aims to protect data confidentiality, integrity and availability.
Cyber security incident	An unwanted/unexpected event, such as an intrusion into a computer system/network, such as the spread of malware.
Cyber security incident report	A report that documents the details of a cyber security incident, such as the type of incident, when it occurred, how it was performed, etc.
Denial of service	An attempt to disrupt a network/business/organisation by issuing more requests than a system is able to cope with, it can be performed with malicious intent or as a protest.
Disaster recovery plan	A plan that documents a set of procedures for an organisation to follow in order to recover and protect a computer system and its data in the event of a cyber security incident.
Encryption	A method that is used to attempt to ensure data security by use of encrypted (secret) code. In order to read the contents of an encrypted message or file, someone must have access to a secret key or password that will enable them to decrypt the message or file.
Escalation of privileges	Exploiting a weakness or weaknesses in an operating system or software application, such as a bug, design flaw or configuration oversight and gaining elevated access to resources that are normally protected.
Ethical hacking	An individual who attempts to penetrate a computer system/network on behalf of its owners for the pur- pose of finding security vulnerabilities that a malicious hacker could potentially exploit. He or she is also known as a white hat hacker. He or she can also work alone.
Firewall	Software that is designed to protect a computer system/network from unauthorised access and intrusion.
Fuzzing	A method that is used to test the security of software.
Hacking	A method of gaining unauthorised access to a computer system/network.
Hacker	An individual who gains unauthorised access to a computer system/network.
Hacktivist	An individual who gains unauthorised access to computer system/network for social or political purposes.
Hoax email	Usually an email message warning recipients of a non-existent threat, usually forging quotes supposedly from authorities such as Microsoft and IBM.
Honeypot	Decoy servers or computer systems that are set up to gather information on intruders or attackers of computer systems/networks.
Host firewall	Software that runs on a single host computer that restricts incoming and outgoing network activity for that host computer only. It can be used to prevent a host computer from becoming infected and stop infected host com- puters from spreading malware to other hosts computers.
Insider	An individual working inside an organisation, a trusted employee, who performs an illegal action, such as hacking.
Integrity	Integrity of data aims to protect data from unauthorised modification.
Intrusion detection system	Software that monitors network or system activities for unexpected or malicious activities.
Intrusion prevention system	Software that examines network traffic flows to detect and prevent vulnerability exploits.
Malware	Software that is designed to cause disruption or damage to data and/a computer system/network.