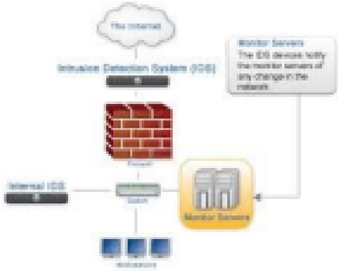
KNOWLEDGE
RGANISE

LO3—Understand measures used to protect against cyber security incidents

Risk Management - does not mean removing all risk, but implementing the following:

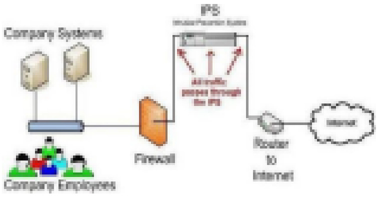
1. identify the risk,
2. measure the risk (how likely is it?, how serious would it be?,
3. monitor and report the risk,
4. control the risk,
5. audit and adjust the risk management process.


The Internet
Intrusion Detection System (IDS)
Monitor Servers
The IDS devices notify the monitor servers of any change in the network
Firewall
Internal IDS
Switch
Monitor Servers
Workstations

Testing and Monitoring Measures

Intrusion Detection System (IDS) is a device or software application that **monitors** a network or systems for malicious activity or policy violations and notifies **Network Intrusion Detection System** (NDIS) e.g. anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

Host Intrusion Detection System (HDIS) are methods of security management for computers, e.g. anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet.



Intrusion Prevention Systems (IPS) are devices or programs that detect attempts at intrusion **and** take action to prevent them.

Biometrics—for our purposes. Means the identification of individuals by using their biological characteristics. These include fingerprints, retinal or iris scans or facial recognition.

Protecting Vulnerabilities — after vulnerabilities have been identified within a system or network, risks are prioritised critical impact to no real damage.

Remediation—is the way vulnerabilities are dealt with. These can be:

- **Patch Deployment**—software code is written to solve a software issues
- **Manual**—network managers/technicians take steps to remove or reduce the vulnerability.
- **Automated Tools**—tools can identify and repair vulnerabilities without human intervention.

Identifying Assets

Hardware Resources – servers, computers, tablets, printers, scanners, plotters, cameras

Software Resources – word processors, databases, spreadsheets, utilities, bespoke software, financial packages etc.

Communication Equipment—hubs, routers, bridges, gateways, modems, cabling, telephone systems.

Information and Data—customer data, employee records, contract data, financial reports, production figures, production costs, sales figures, marketing information

Vulnerability Testing

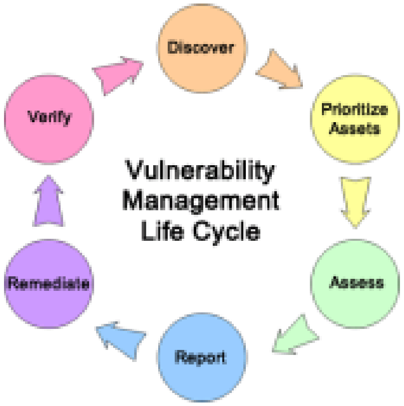
Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the pre-existing flaws in their code and where they are located.

Penetration test, colloquially known as a **pen test**, is an authorised simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.

Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Sandboxing is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs. Sandboxes are used by software developers to test new programming code.

Asset—anything of value owned by an individual or organisation



Cyber Security Controls

The **Physical** control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are:

- Closed-circuit surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- access control cards
- biometric access control systems

Software controls is any computer program designed to enhance information security and defend computers against intrusion (malware) and unauthorized access.

- Firewalls
- Anti-malware
- Operating system updates
- Patch management

IT- Year 12 – Unit 3 – LO3

KNOWLEDGE
R
G
A
N
I
S
E
R

Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text ;* encrypted data is referred to as *cipher text*.

Asymmetric encryption - The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Symmetric encryption - is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Bring your own device (BYOD) refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

RISK—A risk is like a threat, something that could happen but has not yet, that can cause a company to prepare for the eventuality of the risk. For example, a risk assessment form highlights potential risks that can be encountered and planned for but not necessarily acted upon.

- Risks to physical assets include damage, theft, malicious intent, defacing, and redundancy. Some of these can be prepared for, others may have a longer term plan.
- Risks to digital assets include viruses, hacking, corruption and failure to protect from unauthorized internal and external users.
- There is no law in place that says risks need to be defined or prepared for but it is in the company's best interests to prepare.

Procedures and Policies

Acceptable use—how to use computer systems (hardware, software and network) and security measures to obey to protect resources and information.

Digital signature acceptance policy—when and where a digital signature is sufficient evidence of identity for documents.

Email policy—what is appropriate use of the email system and what is not.

Password protection policy—what is an acceptably strong password, e.g. include upper and lower case characters, special characters, at least 8 characters long.

Disaster recovery plan—steps to be taken to recover data, IT systems and application for any incident which could cause a major failure, e.g. terrorist activity, power failure, floods, earthquakes or fire.

User accounts and permission

Remote working— Is the practice of completing your normal daily working life away from the office, using some form of technology and an internet connection.

Cryptography

Is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. In today's computer world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Know it

1. List 3 assets of a computer system and 1 cyber security risk for each.

2. explain the difference between monitoring and controlling systems

3. what do the initials IDS, HIDS, NIDS and IPS stand for?

4. give 4 examples of ways in which physical access to a computer system or network can be controlled.

5. briefly describe 3 different types of control procedures.