# Describe the concepts of security, compliance, and identity (10-15%)

# Describe the capabilities of Microsoft identity and access management solutions (25-30%)

# Describe the capabilities of Microsoft Security solutions (25-30%)

# Describe the capabilities of Microsoft compliance solutions (25-30%)

Cyber Security Concepts

Gain illegal access to computer to cause damage or harm.

Global economic and social disruption

Cyber security – Technology,process and training – helps protect systems, nw, program and data.

Cyber security – Achieve Confidentiality, Integrity and Availability (**CIA**)

**C**onfidentiality – Information visible only to the right people

**I**ntegrity – Information to be changed by the right people or processes

**A**vailability – Information must be visible and accessible whenever needed

Threat Landscape – Email, Social Media acc, Mobile devices, Tech infra, Cloud services, People

Malware – Malicious + Software. Software used by cyber criminals to infect systems and carry out actions

Malware – Steals data. Disrupts normal usage and processes.

Malware components – Propagation (How it spreads) and Payload

**Propagated as below – 3 types**

Malware -> Virus, Worms, Trojans

Virus – Means of entry required, can cause harm once inside.

Worm – No user action required. Worm finds vulnerable systems. Spreads to other systems.

Trojan – Pretending to be genuine. Secretly performs malicious actions like stealing information.

**Payloads as below – 4 types**

Malware – Ransomware, Spyware, Backdoors, Botnet

Ransomware – Locks systems, asks ransom. Encrypts

Spyware – Spies on devices. Keyboard scans, collecting passwords and transmitting back to attacker

Backdoor – Bypass existing security measure via exploit. Hiding malicious code in software. This is backdoor

Botnet – Group of infected devices. Like crypto miners

**Mitigation Strategies – 4 types**

MFA, Browser Security , User education, Threat intelligence,

MFA – Multiple forms of identification.

Browser security – Uptodate, unauthorized extension removal,, block sites

Education – Training

Threat intelligence – Policies for security devices, user access and more.

Cryptography -

Encryption – combine large random prime numbers to create keys.

Asymmetric Encryption – public and private keys

UserA and UserB has public keys

UserA uses UserB’s public key and encrypts. UserB uses its private key to decrypt.

Types of Encryptions –

**DES** Data Encryption Standard, **Triple DES**. – one of the first symmetric encryption std.

**AES** Advanced Encryption Standard – Replaced DES

**RSA**. – One of the first asymmetric encryption standard

Hashing – Verifying data like documents and images and see if it’s tampered with.

Hashing uses algorithm known as hashing function.