1.3 Lesson: Key Concepts and Terminology

1. **Cybersecurity**: The practice of protecting systems, networks, and programmes from digital attacks that aim to access, change, or destroy sensitive information.
2. **Malware**: Malicious software designed to disrupt, damage, or gain unauthorised access to computer systems. Common types include viruses, worms, trojans, and ransomware.
3. **Phishing**: A fraudulent attempt to acquire sensitive information such as usernames and passwords by masquerading as a trustworthy entity in electronic communications.
4. **Firewall**: A security device or software that monitors and controls incoming and outgoing network traffic based on decided security rules, acting as a barrier between trusted internal networks and untrusted external ones.
5. **Encryption**: The process of converting information into a code to prevent unauthorised access during transmission or storage. This ensures confidentiality and integrity of data.
6. **Intrusion Detection System (IDS)**: A device or software application that monitors network or system pursuits for malicious actions or policy violations and alerts administrators when detected.
7. **Incident Response**: The systematic approach taken by an organisation to prepare for, detect, contain, and recover from cybersecurity incidents.
8. **Vulnerability**: A weakness in a system that can be exploited by a threat actor to gain unauthorized access or cause harm.
9. **Threat Actor**: An individual or group that seeks to infiltrate or compromise cyber environments for malicious purposes—this may include hackers, cybercriminals, hacktivists, state-sponsored actors etc.
10. **Two-factor Authentication (2FA)**: A security process in which the user provides two different authentication factors to verify their identity; typically something they know (password) plus something they have (a mobile device).

11. **Data Breach**: An incident where confidential data is accessed without authorisation often leading to the exposure of personal information such as social security numbers or credit card details.
12. **Patch Management**: The process of managing updates for software applications and technologies; crucial for closing vulnerabilities before they can be exploited by cybercriminals.
13. **Security Information and Event Management (SIEM)**: Software solutions that aggregate security data from across an organization's technology infrastructure in real time for analysis—used for monitoring potential incidents.
14. **DDoS Attack (Distributed Denial-of-Service)**: A malicious attempt to disrupt the normal functioning of a targeted server by overwhelming it with traffic from multiple sources simultaneously.
15. **Zero-day Vulnerability**: A previously unknown vulnerability in software that developers have not yet had time to address with a fix; poses significant risk until patched properly.
16. **Social Engineering**: Psychological manipulation techniques used by attackers to trick individuals into divulging confidential information through deception rather than technical means.
17. **Network Security**: Measures taken at the network level designed to protect usability and integrity while safeguarding against threats aimed at both hardware/software within infrastructures.
18. **Endpoint Security**: Strategies used specifically at end-user devices like computers—designed mainly around defending points of entry from external threats within corporate networks.
19. **Risk Assessment:** The systematic process employed organizations evaluate their cybersecurity risks involving identifying potential hazards paired against overall practices affecting response measures towards them protecting assets accordingly.

20 . **Cyber Hygiene***:* Regular practices one follows aiming maintaining consistent good behaviours taking precautionary actions avoiding pitfalls regarding online safety maintaining protection robustly might involve employing updated tools methods limit vulnerabilities arise.