Foundations of Cybersecurity

Module 1

Cybersecurity:

Cyber security is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorised access or criminal exploitation by threat actors.

Threat Actor:

A threat actor is any person or group posing a security risk.

Roles of Security Teams

- Protecting against internal or external threats.
- Helping mitigate threats.
- Ensuring compliance with laws, guidelines, and security frameworks.
- Maintaining business continuity and productivity in case of incidents.
- Reducing cost associated with vulnerabilities and risks.
- Maintaining brand trust.

Internal Threat:

A threat or risk that comes from within a group or organisation rather than from outside, like current or former employees, vendors or trusted partners.

External Threat:

A threat or risk that comes from outside a group or organisation rather than from inside.

Accidental Threats:

Accidental threats are risks that arise from unintentional actions. These threats typically occur due to human error, software bugs, system failures, accidentally deleting important files, misconfiguration security settings, or inadvertently sharing sensitive information, procedural errors, or a degree of negligence.

Intentional Threats:

Intentional threats are risks or dangers that arise from deliberate actions or malicious intent within a system or organisation.

Common Cybersecurity Terminology

Compliance:

Adherence to internal standards and external regulations like laws and security frameworks to avoid security risks, vulnerabilities, and fines.

Security frameworks:

Guidelines used for building plans to help mitigate risks and threats to data and privacy.

Security Controls:

Safeguards designed to reduce specific security risks. Used with security frameworks to establish a strong security posture.

Security Posture:

Organization's ability to manage defence of critical assets and data in case of a security incident.

Network Security:

Practice of securing an organisation's network infrastructure from unauthorised access. This includes data, services, systems, and devices that are stored in an organisation’s network.

Transferable skills:

Transferable skills are versatile abilities acquired in one setting that can be applied effectively in various contexts like problem-solving, critical thinking, attention to detail, communication, adaptability, ethical mindset, teamwork, time management, resilience, and curiosity/continuous learning.

Transferable skills:

Technical skills are specialised abilities and knowledge related to using tools, software, or technologies within a specific field or industry technical skills include programming languages, Security Information and Event Management (SIEM) Tools, Intrusion Detection Systems (IDSs), network security, system administration.

Importance of Security:

Security professionals protect physical and digital assets to manage risks effectively. Security is crucial for ensuring business continuity, maintaining ethical standing, and managing legal implications and moral considerations.

Impact of Data Breaches:

Data breaches affect the organisation's reputation, as well as the lives and reputations of users, clients, and customers. Strong security measures can increase user trust, leading to financial growth and ongoing business referrals.

Personally Identifiable Information (PII):

PII includes information like full name, date of birth, address, phone number, email address, and IP address.

Sensitive PII (SPII):

SPII includes social security numbers, medical or financial information, and biometric data.

Identity Theft:

Identity theft involves stealing personal information for fraud, primarily for financial gain.

Glossary terms from module 1

Terms and definitions from Course 1, Module 1

Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorised access or criminal exploitation

Cloud security: The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorised users

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Network security: The practice of keeping an organisation's network infrastructure secure from unauthorised access

Personally identifiable information (PII): Any information used to infer an individual's identity

Security posture: An organisation's ability to manage its defence of critical assets and data and react to change

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Technical skills: Skills that require knowledge of specific tools, procedures, and policies

Threat: Any circumstance or event that can negatively impact assets

Threat actor: Any person or group who presents a security risk

Transferable skills: Skills from other areas that can apply to different careers