Glossary terms from week 1

Terms and definitions from Course 1, Week 1

Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized 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 authorized 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 organization's network infrastructure secure from unauthorized access

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

Security posture: An organization’s ability to manage its defense 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

---

Revision #1
Created 2023-05-30 17:50:42 UTC by naruzkurai
Updated 2023-06-03 04:51:01 UTC by naruzkurai