Cyber Security: Practice of protecting systems, networks and programs from digital attacks.

**CIA Triad – Cyber security is based on these 3 concepts**

Confidentiality: Sensitive data not authorised

Integrity: Consistency and accuracy and trustworthiness of data

Availability: Consistently and readable accessible for authorise parties.

**Why is cybersecurity important**

The cost of breaches is severe.  
-Loss of customer trust  
-Ransomware  
-Government fines

Ransomware has become very popular in SA, where 80% of targeted individuals were higher education

**Types of Cyber Security**

**Network Security**

**Application security**

**End point security**

**Data security**

**Identity and access management**

**Cloud security:**

**Mobile security**

**Threat Intelligence:** Understanding the threats that hackers use to attack the organisation.

**PWC Cybersecurity Services**

**Strategy, risk and compliance:** Frameworks

**Incident and threat management:** Getting involved with clients to help, research to prepare for incidents.

**Information, governance and privacy:** Ensuring companies apply with privacy laws such as POPIA. With data transfer between countries, you have to follow the laws of wherever the data is.

**Implementation:** Assisting clients with implementing cloud adoption, security

**Managed Services:** Vulnerability management, portfolio management (inform clients which tools/software services they need, and which they can get rid of)

PWC teams can’t both implement and test the code.

**Cyber security careers – there are many 50+**

**Popular Interview questions**

**Threat:** An event with the potential to cause harm

**Theat actor:** An entity that has the Capacity + Opportunity + Intent to cause harm

**Risk:** Vulnerability + Threat (or, Likelihood x Impact)

**Vulnerability:** A characteristic of an entity or system that makes it susceptible to negative impact

**Control:** A measure or action that can be taken to manage risk and confine it ot an acceptable level.

**Demonstration**

Knock client off network.  
When client tries reconnecting, you grab handshake to connect.  
Client then eventually connects none the wiser.  
--In this case, you never interact with router (besides being connected at end)

Poison devices on a network, so when they try logging into a website (HTTP/clear text), the login details are saved to the attacker’s device.