1. Cyber Security is Business Imperative. Discuss

► Cybersecurity is an imperative aspect of modern business operations due to the growing frequency and sophistication of cyber threats. As businesses become increasingly digital, they face heightened expectations from stakeholders to protect sensitive data and maintain trust. Effective cybersecurity is essential not only for safeguarding data but also for ensuring regulatory compliance, managing operational risk, and preserving long-term resilience. Consequently, businesses must strategically invest in cybersecurity measures, balancing costs with the need to protect their reputation and operational integrity.

2a. What is the expression Quantitative Risk Assessment?

► Quantitative Risk Assessment (QRA) involves the use of mathematical expressions and calculations to analyse risk, it is mostly used in Insurance and manufacturing companies.

QRA Breakdown includes:
Profit value (PV) – Properties give competitive advantages that translates to money.
Cost to Maintain (CM)
Cost to Replace (CR)
Cost to Acquire or Develop (CAD)
Cost if Unavailable (CU)
Liabilities if Compromised (L)

Quantitative Analysis (Annualized Loss Expectancy (ALE)) is expressed as:
ALE = Single Loss Expectancy (SLE) X Annualized Ratio of Occurrence (ARO)

Redundant Section (not necessarily included in answer)
where: SLE = AV (Asset Value) x RE (Risk Exposure)
where: AV = PV + CAD + CM + CR + CU + L
where PV = initial profit – current calculated profit.

2b. Why should you consider unauthorized vulnerability scan an attack?

► There's always a malicious intent behind the scan, whoever is scanning is deliberately looking for a weakness in your security posture and will most likely take advantage of it. (simple answer, expatiate as needed)

c. Itemise the estimate likelihood categories

3a. Discuss the story of Robert Fortune

► Robert Fortune was the perpetrator of what author Sarah Rose calls, **"the greatest single act of corporate espionage in history"**. Robert Fortune was a Scottish botanist and adventurer credited with the introduction of tea to India. In 1843 Robert journeyed to China under the employ of the Royal Horticultural Society where he discovered that green and black teas were derived from the same plant. United Kingdom has a great interest in tea which dated back over 200 and only china produced tea and the price was high and this made the British empire to seek better financial alternatives. Fortune's discovery spurred great interest by the British east India Company who saw it as an opportunity to surpass china as the world primary tea producer. Tea production was considered state secret in china and it was illegal to export tea plants for cultivation. The British employed Fortune to infiltrate a tea plant in china with a mission to return to India with sufficient quality and quantity of tea and the manufacturing process of the tea. Fortune gained access to a tea plant in china under a disguise where he discovered and documented the tea manufacturing process. He also discovered that the Chinese were adding Iron cyanide and gypsum to produce a green tint to the tea which was toxic. Robert reported this information to the British and it was used to implicate Chinese as suppliers of unhealthy product while the British on the other hand were able to produce the tea without toxins. The Chinese monopoly was broken and hence the British company controlled the market.

3b. Itemise 5 questions you need to ask yourself about "Who wants to be your Fortune?"

- What are his objectives?
- Do you know the "Robert Fortune" looking at your company?
- What method will he use to achieve them?
- How can you thwart him?
- How can you mitigate your risks?

3c. Itemise vulnerabilities checklists

- **Cyber Espionage, Theft, Exploitation**
  Do you have intellectual property you need to protect?
  Do you have back-ups of your information?
  Are your computer systems connected to the internet?
  Do you store intellectual property and trade secret on a computer?
  Do you use data feed from other sources into your network?

- **Technical Risk**
  Have your business ever been hacked?
  Have you ever found malicious codes in your system?
  Is your network been probed by outside entities?
  Do you store data in the cloud?
  Do you allow remote access to your networks?

- **Human Risk**
  Spear Phishing and whaling
  Email queries
  Ignorance
  Curiosity
  Stupidity

4a. Discuss the various risk decisions

- Mitigation – Involves fixing the deficiency that creates vulnerability
- Transfer – Transferring risk to another part e.g Insurance
- Accept – Accept risk if it's not of high impact or if cost to mitigate risk is high compared to asset you're protecting
- Avoid – Stop doing what exposes you to risk e.g practice of removing vulnerable devices from system.

  (further discuss on each of them)

4b. Who are Hacktivist? How can substandard products and services be a source of cyber threat?

- Hacktivist are groups of hackers or other computer savvy individuals who use their skills to promote social or political agendas.
- Substandard products and services are a source of cyber threat because poorly designed, counterfeit, or antiquated products can introduce vulnerabilities into a business system. Additionally, substandard service such as improper maintenance ans unqualified IT support can lead to misconfigurations or failures that expose systems to attack.

4c. Discuss the idea of previous hacking incidents

- Organizations that have been hacked are likely to face other hacking attempts.
- Hackers like showcasing their successful hacks to peers
- Hackers/Hackings leave backdoors in systems.
- Hackers are careful and leave no trace behind

(further discuss on this)

5a. Discuss the idea of technical risk.

- Technical risks arise from flaws or weaknesses in hardware, software, networks, or system configurations that can be exploited by cyber threats. Examples include outdated software, unpatched vulnerabilities, weak passwords, unsecured cloud storage, or misconfigured firewalls. These risks can lead to data breaches, system failures, or unauthorized access.

5b. How can lack of leadership make you vulnerable?

- Neglecting Training: Failing to prioritize cybersecurity awareness, leaving employees unaware of threats like phishing.
- Ignoring Policies: Exempting themselves from security protocols (e.g., skipping updates or using weak passwords), setting a bad example.
- Underinvesting: Not allocating resources for modern defences, audits, or skilled IT staff.
- Lack of Accountability: Allowing lax enforcement of security measures, increasing negligence.

5c. What are Password Best Practices?

- Make it password you can remember
- Never share password with anyone
- Use maximum strength password that your system allows
- Change password often
- Don’t make it easy to figure out
- Don’t use close relation identity or names as passwords
- Don’t use commonly used or exposed password e.g password, 123456789 e.t.c