Last Semester Mid Q&A

Q1

a) A hacker gains unauthorized access to the control system of a power grid in Dhaka, causing a temporary blackout in several areas. The hacker used stolen credentials to infiltrate the system. Under the **Cyber Security Act, 2023**, what penalties could the hacker face for unauthorized access to a Critical Information Infrastructure (CII) system? **(5 marks)**

b) Discuss the legal implications and potential consequences of such an act on national security and public safety. **(5 marks)**

Answers:

Q1(a) – Hacker in Power Grid

Case:

- Hacker used stolen credentials to access Dhaka's power grid.
- Caused temporary blackouts.

Law (CSA 2023):

- Protects **Critical Information Infrastructure (CII)**.
- Unauthorized access to CII is a punishable cybercrime.

Offence:

- Unauthorized access.
- Cyber sabotage (since blackout occurred).

Punishment:

- Up to **14 years imprisonment**.
- If severe harm: **life imprisonment + fine**.

Conclusion:
The hacker is guilty of cyber sabotage under CSA 2023 and faces up to life imprisonment.

Q1(b) – Implications of Grid Attack

National Security:

- Power grid disruption affects defense, police, and communication.

Public Safety:

- Blackouts → hospital disruption, traffic accidents, panic.

Economic Impact:

- Factories, banks, and trade halted.

Legal Angle:

- CSA 2023 treats this as cyber terrorism/sabotage.
- Maximum punishment applies.

Conclusion:
Such attacks threaten **security, economy, and public trust**, making them one of the gravest cybercrimes.

Q2

a) A financial institution in Chattogram experiences a data breach where sensitive customer information, including bank account details and personal identification numbers, is stolen and sold on the dark web. What are the legal responsibilities of the financial institution under the **Cyber Security Act, 2023**, in terms of reporting the incident and implementing security measures? **(5 marks)**

b) What penalties could the perpetrators face for the data breach, and how does the Act aim to protect affected individuals? **(5 marks)**

Answers:

Q2(a) – Bank Data Breach

Case:

- Financial institution in Chattogram breached.
- Customer data sold on dark web.

Law (CSA 2023):

- Banks = *Essential Service Operators*.
- Must ensure cyber protection.

Responsibilities:

1. **Report incident** to CSA.
2. **Secure systems** (firewalls, encryption).
3. **Notify customers** and take remedial action.
4. **Regular audits & accountability**.

Conclusion:
The bank is legally bound to secure, report, and protect customer data.

Q2(b) – Perpetrator & Victim Rights

For Hackers (Perpetrators):

- Punishment: **Up to 10 years imprisonment + fines**.
- More if used for fraud/identity theft.

For Customers (Victims):

- Must be **informed immediately**.
- Compensation may be provided.
- Law ensures **data privacy rights**.

Conclusion:
Hackers get punished, while customers' rights are safeguarded under CSA 2023.

Q3

a) An individual launches a ransomware attack on a hospital's information system in Sylhet, encrypting patient records and demanding a ransom for their release. The attack disrupts critical medical services. How does the **Cyber Security Act, 2023**, address cyberattacks on Critical Information Infrastructure (CII) systems? **(5 marks)**

b) What are the prescribed penalties for such offenses, and what steps should the hospital take in response to the attack to mitigate damage and comply with the Act? **(5 marks)**

Answers:

Q3(a) – Hospital Ransomware

Case:

- Ransomware encrypted Sylhet hospital data.
- Patient services disrupted.

Law (CSA 2023):

- Hospitals = **Critical Information Infrastructure**.

Offence:

- Unauthorized access.
- Extortion (ransom demand).
- Cyber sabotage (healthcare disruption).

Conclusion:
CSA 2023 classifies hospital ransomware as **serious cyber sabotage**.

Q3(b) – Penalties & Hospital Duties

Penalties for Attackers:

- Up to **14 years or life imprisonment**.
- Heavy fines.

Hospital Duties:

1. **Report immediately**.
2. **Preserve digital evidence**.
3. **Notify patients**.
4. **Activate response team**.

Conclusion:
Attackers face life terms; hospitals must act lawfully and responsibly.

Q4

a) A company operating a national financial exchange fails to implement adequate cybersecurity measures, resulting in a significant financial loss due to a cyberattack. The company had not conducted regular risk assessments or reported previous cybersecurity incidents. What are the requirements for CII operators under the **Cyber Security Act, 2023**, regarding security measures and incident reporting? **(5 marks)**

b) What penalties could the company face for non-compliance with these requirements, and how can they improve their cybersecurity posture to prevent future incidents? **(5 marks)**

Answers:

Q4(a) – Negligence of Financial Exchange

Case:

- Exchange hacked, huge losses.
- Found: no cybersecurity measures.

Law (CSA 2023):

- CII operators must ensure:
    1. Risk assessment.
    2. Preventive controls.
    3. Incident reporting.
    4. Regular audits.

Conclusion:
Failure = corporate negligence under CSA, making them liable.

Q4(b) – Consequences & Prevention

Consequences:

- Fines, license suspension.
- Executive liability.

Preventive Measures:

1. Cybersecurity framework.
2. Staff training.
3. Continuous audits.
4. Cooperation with CSA.

Conclusion:
CSA punishes negligence but also directs prevention for resilience.

Q5

a) A financial analyst named Rahim works for a major bank in Bangladesh. One evening, Rahim uses his personal laptop to access the bank's internal network without authorization. He retrieves sensitive customer data, including account numbers and balances, and saves it on his personal device. Rahim intends to use this information to analyze customer spending patterns for a personal project.

- Was a cybercrime committed by Rahim? If yes, identify the crime under the **Cyber Security Act, 2023**.
- Specify the section under which this crime falls.
- What are the penalties prescribed for this crime under the specified section? **(5 marks)**

b) A software developer named Ayesha is frustrated with her employer, a company that manages critical infrastructure for the national power grid. In retaliation, she introduces a piece of malware into the company's control systems, causing a temporary disruption in power supply to several regions. The disruption lasts for a few hours before the company's IT team can neutralize the malware and restore normal operations.

- Was a cybercrime committed by Ayesha? If yes, identify the crime under the **Cyber Security Act, 2023**.
- Specify the section under which this crime falls.
- What are the penalties prescribed for this crime under the specified section? **(5 marks)**

Answers:

Q5(a) – Rahim (Bank Employee)

Case:

- Accessed bank system with personal laptop.
- Copied customer data.

Law (CSA 2023):

- Unauthorized access = offence.
- Data theft = punishable.

Punishment:

- **7–10 years imprisonment + fines**.

Conclusion:
Rahim committed cybercrime under CSA → liable for up to 10 years in prison.

Q5(b) – Ayesha (Malware in Grid)

Case:

- Inserted malware in power grid.
- Electricity disrupted.

Law (CSA 2023):

- Power grid = CII.
- Malware = cyber sabotage.

Punishment:

- **14 years or life imprisonment + fines**.

Conclusion:
Ayesha committed **cyber sabotage** → faces life imprisonment under CSA.