U-1 (CSDF)

Q1- Cybercrime & Type-

↓

any act of commission committed on or via or help of internet & computer devices.

- can be comitted in opposition to an indivial or a group / govt / private organizations.
- cause direct harm / indirect harm.
- causes loss in Billions each year.

✱ Types of Cyber crime -

1) Crime Against Individual
   a) email spoofing & other online frauds
   b) phishing, spear phishing
   c) spamming
   d) cyber defamation
   e) cyberstalking & harassment
   f) computer sabotage
   g) Pornographic offenses
   h) Password Sniffing.

2) Crime Against Property

3a) Crime Against Government
   b) Credit Card Frauds
   c) Intellectual property crimes
   d) Internet time theft.

Cyber extortion.
- → cyber blackmail.
- → Database ransome attacks.
- → Denial of Service (DOS)
- → Ransomware.

DOMS | Page No.
Date / /

Q2 Process of security risk analysis -

Q9

→ review of risks associated with action or event
→ regular basis & updated to identify new potential
→ strategic risk analysis → min future risk & dang

Steps -

1) conduct a risk assessment survey -
2) Identify risks.
3) Analysis of risks.
4) Develop a risk management plan.
5) Implement risk mangemant plan.
6) Monitor the risks.

Q3 Need for Info. Security.

Information system → consider availble countermeasures or controls stimulated through uncovered vulnerabil

principle of Info security → 1) confidentially 3) Non-Repudiation
2) Authentication 4) Integrity

Need → 1) Protecting organization's functionality
2) Making apps operate safely
3) safeguarding Inform^n that the company uses & collects.
4) Protecting technological resources in organizations.
5) Data Intigrity.
6) Preventing Data Breaches.

Q4 different threats to Information System.

↙ anything that can take advantage of vulnerability to breach security & negatively alter, erase, harm objection or objects of interest.

Software Attacks → Viruses, Worms, Trojan Horses.
↳ Malware, virus, bots, worms.
malicious software.

- Malware → Malicious Software.
- Phishing Attacks.
- Insider Threats.
- Denial of Service (DOS) & Distributed Denial of Service (DDOS)
- Unauthorized Access.
- Physical Threats.
- SQL injection.
- Data Breaches.
- Third Party Attacks.

DOMS | Page No.
Date / /

Q5 Cyber Extortion & Drug Trafficking.

	Cyber Extortion	Drug Trafficking
Nature of crime	• involves using technology to threaten individuals, organization, etc.	• physical world crime, illegal production, distribution etc
Methods	• employ hacking techniques like data breaches or malware to gain access sensitive data.	• physical transportation of drugs across borders or regions.. (drug smuggling)
motivation	• Done for financial gain. ransome in exchange	• financial profit. ↳ from selling drugs.
Payment	• demand payment in Bitcoin ↳ hard to trace transaction	• case or traditional form of currency → illegal procedure
Eg-	• Ransomware attacks. data → encrypted ransom → decryption.	• drug smuggling. borders, region, distributing narcotics in local community

Q7- Nature & Scope of Cybercrime.

- Transitional crime
- without being physically present in location
- only computer & internet needed
- cyberspace → boundaryless world has playground of perpetrators. they commit crimes & remain absent from crime scene.
- Indentification → major challenge.

- Financial
- ~~Financial~~ Data Breach
- Online Harrasment
- Cyber Bullying
- Cyber Terrorism
- Online Scams.
- Hacking