



PCCFM — Prevention of Cyber Crimes and Fraud Management

Complete Book | Table of Contents | 15 chapters + 9 sections

Module A — Cyber Crimes Overview

CH-1	Introduction to Cyber Crime - Concepts and Techniques	2
CH-2	Channels of Cyber Crimes	9
CH-3	Modus Operandi of Cyber Crimes	15
CH-4	Digital Vulnerabilities	22
CH-5	Computer Hackers	30

Module B — Fraud Management

CH-6	Computer Fraud Protection	36
CH-7	Incident Management of Cyber Crimes	43

Module C — Electronic Transactions

CH-8	Online Transactions	50
CH-9	Global Payment Processing	58
CH-10	Electronic Card Frauds	64

Module D — Cyber Laws and Regulatory Compliance

CH-11	Cyber Laws in India	72
CH-12	Electronic Transactions and Taxation Issues	82
CH-13	Human Traits	89
CH-14	Regulatory Compliance	97
CH-15	National and International Institutions	104

Additional Resources

—	Case Studies — Module A: Cyber Crimes Overview	113
—	Case Studies — Module B: Fraud Management	115
—	Case Studies — Module C: Electronic Transactions	116
—	Case Studies — Module D: Cyber Laws and Regulatory Compliance	119
—	Mega Tests — Mega Test 1 — 100 Questions (Full Syllabus)	122
—	Mega Tests — Mega Test 2 — 100 Questions (Full Syllabus)	130
—	Mega Tests — Mega Test 3 — 100 Questions (Full Syllabus)	138
—	Mega Tests — Mega Test 4 — 100 Questions (Full Syllabus)	146
—	Mega Tests — Mega Test 5 — 100 Questions (Full Syllabus)	154

CH-1

Introduction to Cyber Crime - Concepts and Techniques

Topic 1 — Legal Framework for Cyber Cases

- **Base law** — Every cyber case in India is built on the **Information Technology Act, 2000** (as amended).
- **New criminal laws** — It is read with the **Bharatiya Nyaya Sanhita, 2023 (BNS)**, **Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)** and **Bharatiya Sakshya Adhiniyam, 2023 (BSA)**.
- **In force** — The three laws came into force on **1 July 2024**.
- **Replaced** — They replaced the **IPC 1860, CrPC 1973** and **Indian Evidence Act 1872** respectively.
- **Status** — The BNS is an Act in force, not a Bill.

Statute	In force	Role in a cyber case
Information Technology Act, 2000 (as amended)	17 Oct 2000; 2008 amendment from 27 Oct 2009	Defines computer, computer resource, data; civil wrongs (ss. 43, 43A); offences (ss. 65, 66–66F, 67 series); Government powers (ss. 69, 69A, 69B, 70, 70A, 70B); intermediaries (s. 79); extra-territorial reach (s. 75)
BNS, 2023	1 Jul 2024	Penal code: theft (s. 303), criminal breach of trust (s. 316), cheating (s. 318), cheating by personation (s. 319), Forgery incl. electronic record (s. 336), stalking (s. 78), criminal intimidation (s. 351), organised crime (s. 111)
BNSS, 2023	1 Jul 2024	Procedure: FIR irrespective of jurisdiction (Zero FIR, s. 173), search and seizure, production of documents and devices, forensic-team attendance, trial in electronic mode
BSA, 2023	1 Jul 2024	Evidence: electronic records are documents; s. 61 bars refusing admissibility only because a record is electronic; s. 63 governs admissibility with the certificate under s. 63(4)
IPC 1860 / CrPC 1973 / Evidence Act 1872	Repealed 1 Jul 2024	Survive for pre-commencement matters through savings: BNS s. 358, BNSS s. 531, BSA s. 170

Substantive offence law follows the **date of the offence** and the repeal savings. A trial date alone does not decide which procedure or evidence law applies to a pending matter.

- **No 'IT Act 2008'** — There is **no statute called the 'IT Act 2008'**.
- **2008 amendment** — The **Information Technology (Amendment) Act, 2008** amended the 2000 Act. It inserted ss. 43A, 66A–66F, 69A, 69B, 70A, 70B and 79A.
- **Jan Vishwas** — The **Jan Vishwas (Amendment of Provisions) Act, 2023** applies from **30 Nov 2023**. It converted several provisions into monetary penalties and formally omitted s. 66A.
- **DPDP** — **Section 44(2) of the DPDP Act, 2023** will omit s. 43A from **13 May 2027**.

Remember this

- Cite it as: **IT Act, 2000 as amended + BNS / BNSS / BSA, 2023** (in force **1 July 2024**).

Topic 2 — Origin of 'Cyber' and the Meaning of Crime

Term	Origin
Cybernetics	Popularised by Norbert Wiener (1948) ; from Greek kybernetes = steersman / governor (control or regulation). Study of control and communication in machines and living things
Cyberspace	Coined by William Gibson in the short story Burning Chrome (1982) ; popularised in the novel Neuromancer (1984)
Cyber-	Clipped prefix from cybernetics, giving cyberpunk, cybertalk, cyberspace. Working sense: relating to a computer or computer network

- **Crime** — An act punishable by law and treated as a wrong against **public order**. The **State** prosecutes it.
- **Offence** — The wider word. It may be **civil or criminal**.
- **Relation** — Every crime is an offence; not every offence is a crime.
- **Usage** — In practice the two words are used interchangeably.

Remember this

- Gibson → cyberspace; Wiener → cybernetics. A swap of the two is a standard trap.

Topic 3 — Section 43 and Section 66 — Civil and Criminal Tracks

The IT Act splits the same conduct into a **civil track** and a **criminal track**. The technical act is identical; the **mental element** decides the consequence.

Provision	Trigger	Consequence
s. 43 (civil)	Unauthorised access, downloading or copying, introducing a virus, damage, disruption, denial of access, assisting unauthorised access, tampering — done without permission of the owner or person in charge	Compensation to the person affected; no upper cap; claims up to ₹5 crore before the Adjudicating Officer (s. 46)
s. 66 (criminal)	Any s. 43 act done dishonestly or fraudulently	Imprisonment up to 3 years , or fine up to ₹5 lakh , or both
s. 43A (civil)	Body corporate holding sensitive personal data is negligent in maintaining reasonable security practices, causing wrongful loss or gain	Compensation to the person affected; the provision most often applied to banks; omitted from 13 May 2027 when DPDP s. 44(2) takes effect

Two-question test

- **Was it done without authorisation** of the owner or person in charge? If authorised, s. 43 does not apply, however damaging the result (e.g., a **penetration test authorised in writing**).
- **Was it done dishonestly or fraudulently?** If not, it may still fall in s. 43 (compensation) but is outside s. 66 (e.g., an administrator who **deletes a table by mistake**).
- **Disk failure** — A **hard-disk failure** fails both tests.
- **Scope of the test** — The permission and mental-element tests belong to the **s. 43 / s. 66 pairing**. Every other offence is tested on its own statutory elements.

Remember this

- s. 43 = without permission → compensation; s. 66 = same act + dishonest/fraudulent → **3 years / ₹5 lakh**.

Topic 4 — Defining Cybercrime — Tool and Target

- **No definition** — Neither the IT Act, 2000 nor its 2008 amendment nor the BNS defines '**cyber crime**'.

- **What the Act does** — It defines particular acts, contraventions and offences.
- **Working definition** — An offence in which a computer, computer network or other device meeting the statutory definition of a computer is the **tool**, the **target**, or **both**.
- **Liability** — Liability still turns on the statutory elements of each offence.

Role of computer	What the offender wants	Banking illustrations
Tool	Something outside the machine — money, a person, a State	Hacked internet-banking session to move funds; phishing page to cheat a customer; cyber stalking by messaging app; encrypted chat for terror planning; espionage through a compromised laptop
Target	The data or the system itself	Theft of a customer database; ransomware on a core banking server; DoS on a payment gateway; physical theft of a hard disk, pen drive or phone for its data; website defacement
Both	System broken into, then used	Malware on the bank network harvests card data and then uses the bank's own payment channel to withdraw — the classic large banking intrusion

- **Loose synonyms** — **e-crime, electronic offence, online fraud, e-fraud, network fraud, internet crime, remote-access crime, virtual-world fraud, crime in cyberspace** have **no separate legal meaning**.
- **White-collar crime** — It is not a synonym. It is non-violent occupational crime that may or may not involve a computer.

Topic 5 — Statutory Meaning of Computer

- **Section 2(1)(i)** — A **computer** is any electronic, magnetic, optical or other high-speed data processing device or system.
- **Functions** — It performs **logical, arithmetic and memory functions** by manipulating impulses.
- **Includes** — All connected input, output, processing, storage, software and communication facilities.
- **Test** — The test is **function, not appearance**.

Term	Meaning
Computer system [s. 2(1)(i)]	Device or collection of devices with input and output support, usable with external files, containing programs, electronic instructions and stored data
Computer network [s. 2(1)(j)]	Interconnection of computers or devices through communication media — satellite, microwave, terrestrial line, wire, wireless or other channel
Computer resource [s. 2(1)(k)]	Computer, computer system, computer network, data, computer database or software — the widest term , used when a section wants maximum reach

- **Covered devices** — Mobile phones, tablets, PDAs, **PoS terminals, ATMs**, smart-card readers and **IoT devices** with a microprocessor fall inside the definition.
- **Trap** — 'Cybercrime is committed only with a desktop computer' is always wrong.
- **No cyber-court system** — The IT Act creates **no separate nationwide criminal cyber-court system**. Cases follow competent-court jurisdiction and any local designation.
- **What exists** — Specialised policing through **cyber crime cells / wings** of city and district police, and the **Adjudicating Officer** for civil claims.
- **EOW** — Many States investigate economic offences through a dedicated **Economic Offences Wing**.
- **Normal route** — Cybercrime is normally handled by regular policing through the cyber cell.

Topic 6 — Fraud Triangle and the Shift from Cash to Data

A fraud usually needs three conditions together; remove any one and it normally does not happen. The underlying failure is **lack of self-regulation**.

Limb	Content	Control point
Pressure / need / greed	Motive — debt, habit, lifestyle, unmet target, avarice	Outside the bank's control
Opportunity	A control gap that lets the fraud be done and concealed	The only limb the bank fully controls — hence control design is the standard prevention answer
Rationalisation	Self-justification — 'only borrowing', 'the bank owes me', 'everyone does it'	Culture, ethics, awareness

Dimension	Money theft	Data theft
Nature of asset	Static; spent once	Dynamic; converted into money repeatedly and resold to several buyers
Presence	Offender must be there	Normally remote , from another State or country
Effect on original	Asset removed	Asset usually copied — victim still holds it
Detection	Noticed almost at once	May run undetected for months
Means	Weapons, muscle, presence, escape route	Computer, connection, knowledge of the target system
Scale	What can be carried	Size of the database

- **Copied data** — Copied data is not 'taken away' in the strict property sense.
- **IT Act framing** — So the Act treats it as **unauthorised access, downloading and copying (s. 43)** and the offences in **ss. 66 and 66B**.
- **Section 72** — Amended **s. 72** now carries a **monetary penalty** (up to ₹5 lakh).
- **Physical taking** — Taking a laptop, hard disk or pen drive is ordinary **theft under the BNS**, charged alongside IT Act offences.
- **IoT** — The **Internet of Things (IoT)** extends network connectivity to appliances, vehicles, meters, medical and industrial equipment, even livestock.
- **Identifier** — Each device has a **unique identifier** and transfers data without human interaction.
- **Legal status** — An IoT device meeting the functional definition is a computer or part of a computer resource.
- **Entry points** — Building-management systems, CCTV or ATM sensors can be entry points into bank systems.

Topic 7 — History and Measurement of Cybercrime

- **Use dated milestones** — Rely on dated, checkable milestones.
- **1820 loom myth** — The story of an **1820 French loom sabotage** as the 'first cybercrime' is **apocryphal**. A mechanical loom is not a computer.
- **Rolling phrases** — Phrases such as 'computers have existed for seven decades' decay with each reprint.

Date	Incident	Significance
Nov 1988	Morris Worm	Disabled much of the early internet; first conviction under the US Computer Fraud and Abuse Act

Date	Incident	Significance
Oct 1989	WANK Worm (NASA)	Commonly cited first hacker attack — political message, not money
Feb 1999	Military satellite control intrusion (reported, southern England)	Attack on a control system — ancestor of SCADA/ICS concerns
Jan 2000	'Maxim' card extortion (CD Universe)	Template for breach-plus-ransom
Mar 2006	Business-school application-status hack	Ordinary users used a published method — authorisation, not skill , decides criminality
2008	Mass site redirection; supermarket card breach; ISP homepage redirect	Shift to industrialised, volume crime
2000	IT Act, 2000 enacted	Statutory anchor for Indian cybercrime
27 Oct 2009	IT (Amendment) Act, 2008 in force	Modern offence set — 43A, 66–66F, 69A, 69B, 70A, 70B, 79A
1 Jul 2024	BNS, BNSS, BSA in force	Current penal, procedural and evidence base

- **Hard to measure** — In a large breach the loss is unknown at reporting, revised later, and often never published.
- **No 'biggest attack'** — No defensible answer exists to 'the biggest cyber attack'.
- **Survey figures** — Use them only when the **publisher, fieldwork period, geography, sample size and exact question** are stated. Otherwise drop them or label them historical.
- **Nested percentages** — Watch for a share of a sub-group quoted as a share of everyone.

Topic 8 — Conventional Crime and Cybercrime — Evidence

- **Scene and evidence** — A cybercrime **has a scene**, usually several, and **has evidence**.
- **Logs** — Logs are timestamped, retained and hard to alter without trace.
- **Instruments** — Malware, skimmers, card writers and rogue access points are **instruments** seized like any other.
- **Physical acts** — Skimming, shoulder surfing, tailgating and dumpster diving are physical acts that leave physical traces.

Evidence layer	What is found	Who holds it
Endpoint / device	Deleted files, browser and app history, malware artefacts, USB records, geolocation, photos of a card or screen	Victim or accused; imaged forensically before examination
Server and application	Logins, transactions, session IDs, failed attempts, privilege changes, database queries	The bank — log integrity and retention are a control obligation
Network / ICT logs	IP addresses, NAT, DNS, firewall and proxy records, connection times	Organisation and ISP; CERT-In requires logs for a rolling 180 days within Indian jurisdiction
Cloud / service provider	Mailbox contents, file versions, account creation and access, device registrations	Data centres, cloud, VPN and hosting providers on lawful demand; subscriber records kept 5 years after cancellation
Telecom	Call Detail Records (CDRs), tower-location data	Telecom providers on lawful requisition

Evidence layer	What is found	Who holds it
Financial trail	Beneficiary and mule accounts, wallet/PPI hops, card authorisation messages, ATM cash-out points	Banks, payment operators, card networks — often the fastest route to identity
Physical	CCTV, ATM/PoS camera images, skimming and shimming hardware, printouts, access records	Premises and surroundings

Aspect	Conventional crime	Cybercrime
Presence	Offender at the scene	Usually remote , possibly in another country
Skill	Physical capability	Technical knowledge ; muscle irrelevant
Speed and reach	One victim, one place, one time	Thousands of victims, automated, across jurisdictions
Investigation	From the scene outwards	Reconstructs the sequence of events across systems and time
Proof at trial	Physical exhibits	Storage media and printouts with the BSA s. 63(4) certificate
Jurisdiction	Ordinarily clear	Reasoned; s. 75 IT Act covers acts outside India involving a computer system in India
Anonymity	Offender identifiable	Faceless ; identity by attribution work

Topic 9 — Threat, Vulnerability and Risk

Term	Meaning
Threat	A circumstance or event capable of causing harm. Sources may be internal or external, intentional or accidental — insiders, equipment failure, environmental events
Vulnerability	An inherent weakness in the system — no firewall or antivirus, weak password policy, unpatched OS, weak authentication, untrained user
Risk	Likelihood and impact of an adverse event, considering threats, vulnerabilities and existing controls. 'Threat × vulnerability' is only a teaching shorthand

- **Risk treatment** — It reduces likelihood or impact and manages the **residual risk**.
- **Target of treatment** — The motive cannot be controlled, so treatment works on the **vulnerability**.
- **Foreseeable events** — Flood, earthquake or war are **foreseeable risk scenarios** to be planned for in BCP/DR.
- **Force majeure** — It is a contractual concept, not 'impossible to anticipate'.

What is not a cybercrime

Category	What happened	Legal consequence	Banking example
Accident / act of God	No human act aimed at the system	None; insurance, BCP and DR	Flood in data centre; lightning
Control / component failure	System or process failed; no unauthorised act, no intent	None criminal; availability incident, root-cause analysis	Hard-disk crash, UPS failure, batch job not run
Cyber incident	Security event to be responded to and, if specified, reported	Report to CERT-In within 6 hours of noticing	Malware on a server; attempted intrusion; phishing site imitating the bank
Cyber offence	Conduct meeting the elements of a statutory offence	Prosecution under IT Act and BNS; compensation under s. 43 / 43A	Hacked fund transfer; stolen customer database; cheating by personation

Categories overlap: one **ransomware** event is at once a **cyber incident** (CERT-In in 6 hours), a **cyber offence** (FIR) and a **control failure** (root-cause fix). The three tracks are independent.

Topic 10 — Threat Catalogue

Group	Threats	Key meanings
Malicious code	Virus, worm, malware, adware, spam, ransomware, Stuxnet, Zeus	Stuxnet — malware built to damage industrial control equipment, the standard cyber weapon . Zeus — banking trojan stealing credentials from the browser session
Availability attacks	DoS, DDoS, fast flux	DoS floods a service from one source; DDoS from many hijacked machines; fast flux rapidly rotates IP addresses behind a domain so infrastructure cannot be taken down
Network attacks	IP spoofing, email spoofing, session hijacking, man-in-the-middle	Spoofing forges the source (IP or sender) to appear trusted
Application attacks	SQL injection, buffer overflow, cross-site scripting (XSS)	SQL injection passes database commands through an input box; buffer overflow writes past allocated memory to run attacker code; XSS plants a script in a trusted page to run in the victim's browser
Remote access	Spying, remote administration tools, Windows session hijacking	Session hijacking takes over a logged-in session — no password needed
Physical and human	Theft of hard disk, pen drive, PDA or phone; scavenging; shoulder surfing; tailgating; social engineering; personation	Scavenging / dumpster diving : data from discarded devices, paper. Shoulder surfing : reading a PIN over the shoulder. Tailgating : following an authorised person through a secured door. Social engineering : making a person break procedure
Data and card	Card cloning, port sniffers, data diddling, e-forgery, falsification of electronic records	Card cloning copies genuine card data onto another card; data diddling alters data before or during entry; e-forgery creates or alters an electronic record to pass it as genuine
Unknown flaws	Zero-day attacks	Exploit a flaw with no patch yet because the vendor does not know of it — patching alone cannot stop it

Topic 11 — Mens Rea and Motives

- **Mens rea** — The guilty mind: the criminal intent that separates a punishable act from one with the same technical result.
- **Example** — A researcher with **written authorisation** and an intruder may type identical keystrokes when scanning a network. Only the intruder commits a crime.
- **In the IT Act** — Mens rea appears as '**dishonestly or fraudulently**' in s. 66 and as **absence of authorisation** in s. 43.

Motive	Note
Show-off / technological supremacy	Original motive of early hackers and virus writers; matured into malware-for-hire
Greed for money through computerised data	Today the dominant motive
Thirst for publicity	The attack is announced; the announcement is the point
Adventure and inquisitiveness	Experimenting to learn how a system works

Motive	Note
Urge to do the forbidden	Psychological attraction of the prohibited
Desire to cause harm	Destructive intent with no gain sought

- **Ordinary motives** — Enmity, ideology, revenge and lust also apply.
- **Motive meets vulnerability** — Motive alone produces nothing. It becomes risk when it meets a vulnerability (weak authentication, poor password policy, unpatched systems, missing controls).

Topic 12 — Cyber Criminals and Their Classification

- **No legal definition** — There is **no legal definition of a cyber criminal**. Anyone who commits a cybercrime is one.
- **Same in law** — The law draws no distinction from a conventional criminal for trial or conviction.
- **In practice** — He is **faceless and remote** and must stay **technologically ahead** of defenders.
- **Planning** — He first decides the crime and his tools (know-how and devices). He needs **no physical strength**.

By statute charged

Offenders are charged under the **IT Act, 2000**, under other statutes (mainly the **BNS**), or both. The FIR names every applicable section; if one charge fails, the other may still succeed.

Conduct	IT Act, 2000	BNS, 2023
Phishing page collecting card credentials, then a fraudulent debit	s. 43, s. 66, s. 66C identity theft, s. 66D cheating by personation	Cheating (s. 318); cheating by personation (s. 319); forgery of electronic record (s. 336)
Organised gang running mule accounts across States	s. 66, s. 66D and applicable data offences	Organised crime (s. 111) — definition expressly includes cyber-crimes by a syndicate

- **Section 66A** — Struck down in **Shreya Singhal v. Union of India** and omitted. It is never a live offence.
- **Section 79** — Gives intermediaries a **safe harbour** for third-party content. It is lost on failure of due diligence or of acting on lawful orders.
- **Section 79A** — Lets the Central Government notify an **Examiner of Electronic Evidence**.

By target and by method

Target	Examples
Property and assets	Data theft, theft of equipment, phishing, card cloning, scavenging, DoS
Individual person	Cyber stalking, harassment, spying, hacking a personal computer, stealing an email password, privacy violation
Society, nation or group	Cyber espionage, cyber terrorism, attacks on critical information infrastructure, organised hacker groups

By method: (i) **physical theft** of a computer or gadget; (ii) **illegal access** to obtain data; (iii) **hacking and data theft as a profession**, including selling capability for anti-national work.

Seven types

Type	Skill	Distinguishing feature
Script kiddies	Low	Run tools written by others; succeed only against weak systems — defined by lack of skill, not lack of harm
Spammers	Low–medium	Bulk unsolicited mail; often the delivery channel for phishing and malware
Hacker groups	High	Anonymous, build tools, hack for no criminal reason, sometimes hired to test security — authorisation, not skill , decides criminality
Phishers	Medium	Obtain account numbers, user names, passwords via fake sites and messages — attack the person , not the system
Political / religious / commercial groups	High	Attack for ends other than direct gain; Stuxnet is the standard example
Insiders	Varies	Legitimate access makes detection hard
APT agents	Very high	Highly targeted, organised, usually State-sponsored ; defined by persistence — months of dwell time

The '20% of threats, 80% of damage' insider ratio has **no reproducible source**. Insider risk has three populations, each needing its own control:

Insider	Profile	Control
Malicious	Intends harm	Monitoring
Negligent	Ignores or bypasses control without meaning harm	Training and control design
Compromised	Credentials driven by an external attacker; may be a victim	Multi-factor authentication and anomaly detection

- **Neutral technology** — Technology is **nation-neutral and religion-agnostic**. A network connection is the only prerequisite.
- **Cyber gangs** — Members who never meet coordinate across borders.
- **Crimes supported** — Drug trafficking, counterfeit currency and hawala, contraband, human trafficking, arms peddling, cyber terrorism and anti-national activity.
- **Same method** — The mission differs; the modus operandi is the same.

Remember this

- Insiders: malicious → monitoring; negligent → training; compromised → MFA + anomaly detection.

Topic 13 — Institutions and Reporting

Clocks

Body	Basis	Mandate	Does not
CERT-In	s. 70B IT Act	National nodal agency for incident response — collection, analysis, alerts, emergency response; binding directions on reporting and logs	Investigate or prosecute
NCIIPC	s. 70A IT Act	Protection of Critical Information Infrastructure — systems whose incapacitation debilitates national security, economy, public health or safety	Handle ordinary consumer cybercrime
I4C	MHA (attached office from 1 Jul 2024)	Coordinates cybercrime response across States; runs the National Cyber Crime Reporting Portal and helpline 1930	Register or try cases
Cyber Swachhta Kendra	Under CERT-In	Botnet cleaning and malware analysis; free removal tools	Act as reporting or enforcement channel
Adjudicating Officer	s. 46 IT Act	Civil claims up to ₹5 crore; above that, competent court	Try an offence
Police cyber cells	BNSS, 2023	FIR, investigation (IT Act offences by officer not below Inspector , s. 78), arrest, chargesheet	Regulate
INTERPOL	Own Constitution; 196 members	Cooperation and information exchange through National Central Bureaus	Arrest — national police arrest

CERT-In directions under s. 70B(6)

- Report a specified cyber incident within **6 hours** of **noticing it or being brought to notice** — the clock starts at knowledge, not at breach or confirmation.
- Maintain ICT system logs for a rolling **180 days** within Indian jurisdiction; synchronise clocks with **NIC / NPL NTP** servers.
- Data centres, VPS, cloud and VPN providers keep subscriber records for **5 years** or longer after cancellation.
- Non-compliance: imprisonment up to **1 year** or fine up to **₹1 crore**, or both [s. 70B(7)].
- Separate clocks run for RBI reporting (on **DAKSH** within **6 hours** of detection), customer notification and law-enforcement referral; one filing does not discharge another.

Example: Incident noticed at **07:05** → CERT-In report due by **13:05** the same day, even if the intrusion began two days earlier.

Customer side — the golden hour

- Call 1930** — Call **1930** (24×7) at once and lodge the complaint on the National Cyber Crime Reporting Portal.
- Why early** — Early reporting lets funds be frozen in the mule chain.
- RBI framework** — Liability under the RBI framework on limiting customer liability in unauthorised electronic banking transactions:

Situation	Customer liability
Bank's own fault (contributory fraud, negligence, deficiency)	Zero , whenever reported
Third-party breach, reported within 3 working days	Zero
Third-party breach, reported in 4–7 working days	Lower of transaction value or cap. ₹5,000 (BSBD). ₹10,000 (other SB, prepaid cards, credit cards up to ₹5 lakh limit, current/CC/OD of MSMEs and individuals up to ₹25 lakh). ₹25,000 (other current/CC/OD, credit cards above ₹5 lakh)
Third-party breach, beyond 7 working days	As per board-approved policy
Customer negligence (e.g., sharing credentials)	Entire loss until reported to the bank

- Shadow credit** — The bank must **shadow-credit** within **10 working days** of notification, without waiting for insurance.
- Resolution** — The bank must resolve the case within **90 days**.
- From 1 January 2027** — A revised framework applies.
- Zero liability** — For a third-party breach reported within **5 calendar days** (to the bank and on the portal / 1930).
- Timelines** — Resolution in **45 days** (**60 days** cross-border).
- Small frauds** — One-time compensation for frauds up to **₹50,000**: **85% of net loss** or **₹25,000**, whichever is lower.
- Alerts** — Instant SMS alerts above **₹500**.

Example: Regular SB account, third-party breach, reported on the 5th working day, unauthorised debit ₹14,000 → liability = lower of ₹14,000 and ₹10,000 = **₹10,000**; the bank bears ₹4,000.

Data protection and international status

- DPDP** — The **Digital Personal Data Protection Act, 2023** works with the **DPDP Rules, 2025** (notified **13 Nov 2025**).
- Phase 1** — Institutional provisions apply on publication.
- Phase 2** — Consent Manager provisions apply **one year** later (**13 Nov 2026**).
- Phase 3** — Core processing obligations and s. 44(2) apply **18 months** later (**13 May 2027**).
- Status** — It is neither 'fully in force' nor 'still a Bill'.
- UN Convention** — The **UN Convention against Cybercrime** is open for signature. India signed it in **September 2026**.
- Entry into force** — **90 days** after the **40th** ratification. It is **not yet in force**; signature is not ratification.
- No single framework** — Neither it nor the Budapest Convention is a single global framework.
- INTERPOL** — INTERPOL is not a global police force.

Remember this

- CERT-In: **6 hours** from noticing; logs **180 days**; subscriber records **5 years**.
- Liability now: 3 / 4–7 / beyond 7 working days; shadow credit 10 working days; resolve in 90 days.

Topic 14 — Classifying an Incident —

Applied Case

- Discovery** — At **07:05** on Monday a bank finds an unknown process on a card-management server, running since Friday night.
- Intrusion** — A contractor's credentials were used from abroad and card data was copied out.
- Same window** — A hard disk in a reporting server failed, losing a day of MIS reports.
- Root cause** — The contractor had opened a phishing mail.

Step	Analysis
Separate events	Hard-disk failure = availability / control failure ; backup, restore, root-cause — not a cybercrime, not the reportable incident. Data exfiltration = cyber incident and cyber offence , run in parallel
Reporting clock	CERT-In report due 13:05 (6 hours from noticing), not from Friday's intrusion or the end of investigation; RBI, customer and police clocks run separately
Offender	Contractor is a compromised insider ; preventive control is MFA and anomaly detection , not discipline. An APT label needs evidence of sophisticated capability, resources and sustained objectives
Charges	IT Act s. 43 (compensation), s. 66 (offence), s. 43A if the bank's security practices were inadequate; BNS general offences and organised crime if a syndicate is shown; s. 75 covers the act done from abroad
Evidence	Server and application logs, ICT logs (180 days), contractor's imaged laptop, cloud records, card-misuse financial trail, CCTV; printouts with the BSA certificate

Topic 15 — IT Act Sections to Memorise

Section	Provision	Consequence
2(1)(i)	Computer	Function-based; covers phones, tablets, PoS, ATMs, IoT
2(1)(k)	Computer resource	Widest term
43	Unauthorised access, download, virus, damage, denial, tampering	Civil — compensation
43A	Negligent body corporate — sensitive personal data	Compensation (until 13 May 2027)
46	Adjudicating Officer	Claims up to ₹5 crore ; above — competent court
65	Tampering with computer source documents	Up to 3 years or fine up to ₹2 lakh , or both
66	s. 43 act done dishonestly or fraudulently	Up to 3 years or fine up to ₹5 lakh , or both
66B	Dishonestly receiving stolen computer resource or device	Up to 3 years or fine up to ₹1 lakh , or both
66C	Identity theft — another's electronic signature, password, unique ID	Up to 3 years and fine up to ₹1 lakh
66D	Cheating by personation using a computer resource	Up to 3 years and fine up to ₹1 lakh
66E	Violation of privacy — private images	Up to 3 years or fine up to ₹2 lakh , or both
66F	Cyber terrorism	Up to imprisonment for life
69 / 69A / 69B	Interception, monitoring, decryption; blocking; traffic-data monitoring	Failure to assist under s. 69: up to 7 years and fine; encryption itself is not an offence
70 / 70A / 70B	Protected system; NCIIPC; CERT-In	Unauthorised access to protected system: up to 10 years and fine; CERT-In directions: 6 hours, 180 days
72	Breach of confidentiality by a person with powers under the Act	Penalty up to ₹5 lakh
75	Extra-territorial application	Offence outside India by any person involving a computer system in India
79 / 79A	Intermediary safe harbour; Examiner of Electronic Evidence	Safe harbour lost on failure of due diligence or a lawful order

Remember this

- 66C and 66D: 3 years **and** ₹1 lakh (both mandatory); 66 and 66E: **or** / both.

PCCFM | Module A | CH-1 | MCQs

Q1. A fraudster hosts a fake internet-banking page, captures a customer's credentials and debits her account. Which IT Act section specifically covers cheating by personation using a computer resource?

- (a) Section 66B (b) Section 66E (c) Section 66D (d) Section 65

Q2. A bank's IT team, under a written mandate, runs a vulnerability scan that accidentally slows a server. Under the IT Act this is:

- (a) Not a contravention, as the act was authorised
(b) A section 66 offence, as a computer resource was disrupted
(c) A section 43A breach by the bank as body corporate
(d) Cyber terrorism under section 66F

Q3. A database administrator, acting within his authorised role, deletes a production table by mistake. Which statement is correct?

- (a) He is liable under section 66 for damage to data
(b) He commits identity theft under section 66C
(c) He is guilty of tampering under section 65
(d) He is outside section 66, as there is no dishonest or fraudulent intent

Q4. A bank notices a specified cyber incident at 21:40 on Tuesday, though logs show the intrusion began on Sunday. The CERT-In report is due by:

- (a) 21:40 on Wednesday
(b) 03:40 on Wednesday
(c) Six hours after the forensic report is complete
(d) 03:40 on Monday

Q5. A hard disk in a bank's reporting server crashes and a day's MIS reports are lost. The event is best classified as:

- (a) A cyber offence under section 66
(b) A cyber incident reportable to CERT-In
(c) An availability and control failure
(d) Data diddling

Q6. Ransomware encrypts a bank's core servers. Which response set is correct?

- (a) Only an FIR, since it is a crime
(b) Only a CERT-In report, since it is an incident
(c) Only root-cause analysis, since it is a system failure
(d) CERT-In report within 6 hours, FIR, and root-cause analysis, all in parallel

Q7. A PoS terminal at a merchant outlet is tampered with to capture card data. Is the terminal a 'computer' under the IT Act?

- (a) Yes, because the definition is based on function, not appearance
(b) No, only desktop and laptop machines qualify
(c) No, it is a payment device regulated only by the RBI
(d) Yes, but only if notified as a protected system

Q8. A hacker sitting in another country breaches a bank server located in Pune. Which provision applies the IT Act to him?

- (a) Section 79 (b) Section 46 (c) Section 75 (d) Section 70A

Q9. A contractor's credentials are hijacked after he opens a phishing mail and are used to copy card data. Which control would most directly have prevented this?

- (a) Disciplinary action against the contractor
(b) Faster CERT-In reporting
(c) Insurance cover for cyber losses
(d) Multi-factor authentication with anomaly detection



Q10. In the fraud triangle, which limb is fully within the bank's control?

- (a) Opportunity (b) Pressure
(c) Rationalisation (d) Greed

Q11. In a new criminal proceeding, a bank produces server log printouts. The certificate for admissibility of these electronic records is governed by:

- (a) Section 65B of the Indian Evidence Act, 1872
(b) Section 63 of the Bharatiya Sakshya Adhiniyam, 2023
(c) Section 79A of the IT Act, 2000
(d) Section 173 of the BNSS, 2023

Q12. A complainant asks police to register a case under section 66A for an offensive social-media post. The correct position is:

- (a) It carries 3 years and fine
(b) It needs CERT-In sanction first
(c) It cannot be invoked, as it was struck down and has been omitted
(d) It is now a civil penalty of ₹5 lakh

Q13. A company claims ₹7 crore as compensation for unauthorised access to its systems under section 43. The claim lies before:

- (a) The Adjudicating Officer (b) CERT-In
(c) NCIIPC (d) The competent court

Q14. A data-entry operator alters loan figures before they are keyed in, so the system output is wrong from the start. This is:

- (a) Card cloning (b) Data diddling
(c) Session hijacking (d) Tailgating

Q15. A regular savings-account holder reports a third-party-breach debit of ₹14,000 on the 5th working day after the bank's alert, under the current RBI liability framework. The customer's liability is:

- (a) Nil (b) ₹5,000 (c) ₹14,000 (d) ₹10,000

Answer key

Q	Ans	Q	Ans	Q	Ans	Q	Ans	Q	Ans
1	c	4	b	7	a	10	a	13	d
2	a	5	c	8	c	11	b	14	b
3	d	6	d	9	d	12	c	15	d

CH-2 Channels of Cyber Crimes

Topic 1 — Three Ways to Classify Cyber Crime

- **No official scheme** — There is **no single official or standardised classification** of cyber crime.
- **Three working schemes** — Each is built from the parameters applied while dealing with a case.
- **By victim** — Used by policy makers and criminologists.
- **By legal route** — Used by investigators and courts.
- **By modus operandi** — Used by security teams.
- **Overlap** — An incident usually falls under **one or more** categories, not exactly one.

By victim

Category	What is targeted	Typical examples
Individual	A person; harm is personal rather than financial	Cyber stalking, cyber bullying, defamation on social media, morphing, harassment, identity theft aimed at one person
Property or money	Value — money, data, intellectual property; owner's identity incidental	Card fraud, credential phishing, ransomware, data theft, software piracy, copyright infringement
Group, society or nation	A collective, the public or the State and its infrastructure	Cyber terrorism, attacks on critical information infrastructure, hate campaigns, disinformation, cyber warfare

By legal and investigative route

Route	What it carries
IT Act, 2000 (as amended)	Compensation/penalty provisions and criminal offences; ss. 65–74 are not uniformly criminal after the Jan Vishwas amendments
General penal law	BNS, 2023 for conduct on or after 1 July 2024 (cheating, forgery, criminal breach of trust, extortion, intimidation); IPC 1860 for earlier conduct
Other special Acts	Copyright Act 1957, Trade Marks Act 1999, Companies Act 2013, PMLA 2002, NDPS Act 1985 and sectoral laws, each with its own machinery
Civil law and torts	Compensation, not punishment — defamation as a tort, breach of an outsourcing contract, negligence, s. 43 compensation claims

By modus operandi — the four channels

Channel	How the attacker gets in	Bank example
Physical attack	The hardware is the target — machine, device, media	Skimmer or shimmer on an ATM, pinhole camera over PIN pad, stolen laptop or backup tape, rogue USB, cut leased line
Software attack	Information resource reached through a program — malware, exploit code, malicious script	Ransomware on a branch server, banking trojan on a phone, SQL injection on internet banking, keylogger on a teller PC
Network access	A weakness in the network, with or without a software flaw	DoS/DDoS on the portal, man-in-the-middle on open Wi-Fi, open port or bad firewall rule
Insider threat	Information asset reached through an employee — physically, logically or systemically; employee need not be the criminal	Staff selling customer data, misuse of maker-checker override, leaver copying a database, staff conniving with an outside fraudster

- **Wider than theft** — The insider channel is wider than 'a dishonest employee'.
- **Included** — **Negligence** that opens the path and **systemic misuse of legitimate access** are inside it.
- **Trend** — Insider threats and systems staff conniving with fraudsters are rising in banking. So vigilance and fraud management keep being strengthened.

Remember this

- Victim **3**, legal route **4**, modus operandi **4** (physical, software, network access, insider) — none is an official taxonomy.