

UNIT 2

Cyberattacks, Cybersecurity, and Cyber Law

(12 Hours) — Cyber Law & Professional Ethics (CACS401)

Please read: These notes are prepared as a study aid and **may contain errors** or out-of-date details, especially section numbers, penalties, dates, case names and statistics. Always cross-check with your prescribed textbook, class lectures, and the official text of any law (Nepal Law Commission website) before relying on them in an exam or in practice.

Legal note: section numbers and penalties under Nepal's Electronic Transactions Act (ETA) 2063 were checked against several secondary sources, which do not always agree (for example on the AD year and on the fine under Section 46). Confirm against the official Act before quoting them.

2.1 The Threat Landscape

A **computer incident** is any event that threatens the confidentiality, integrity or availability of information systems or data, or that violates security policy. Incidents range from a single infected laptop to a nationwide ransomware outbreak. An **exploit** is an attack that takes advantage of a vulnerability (a weakness in software, hardware, process or people). A **vulnerability** is the weakness; a **threat** is anything that can exploit it; **risk** is the likelihood and impact of that happening.

Types of Attackers

Attacker	Description / motive
Script kiddie	Low-skill person using ready-made tools, often for fun or fame.
Hacker types	White hat (authorised, ethical), black hat (criminal), grey hat (unauthorised but without malicious intent).
Cybercriminal	Profit motive: fraud, ransomware, theft of card and banking data.
Malicious insider	Employee or contractor abusing legitimate access; the hardest to detect.
Hacktivist	Political or social cause; defacement, DDoS, data leaks.
State-sponsored / APT	Well-funded groups conducting long-term espionage or sabotage (Advanced Persistent Threat).
Cyberterrorist	Aims to cause fear or disruption to critical infrastructure.

Common Types of Exploits

Exploit	Explanation
Virus	Malicious code that attaches to a file/program and spreads when the host is run or shared.
Worm	Self-replicating malware that spreads across networks without user action (e.g., WannaCry 2017 used a Windows flaw).
Trojan horse	Malware disguised as a useful program; often opens a back door.
Ransomware	Encrypts data and demands payment for the key; often combined with data-leak threats.
Spyware / keylogger	Secretly collects user activity, passwords or keystrokes.
Rootkit	Hides the presence of malware and gives privileged access.
Logic bomb	Code that triggers a harmful action when a condition is met (date, deleted account).
Botnet	Network of infected computers ("zombies") controlled remotely, used for spam and DDoS.
DoS / DDoS	Floods a service with traffic so legitimate users cannot access it.
Phishing family	Deceptive email (phishing), targeted email (spear phishing), SMS (smishing), voice calls (vishing).
Social engineering	Manipulating people into revealing secrets or performing actions.
Man-in-the-middle	Attacker secretly intercepts and possibly alters communication between two parties.
SQL injection / XSS	Injecting malicious input into web applications to steal or alter data or run scripts in users' browsers.
Zero-day exploit	Attack on a vulnerability unknown to the vendor, so no patch exists yet.
Password attacks	Brute force, dictionary attack, credential stuffing.

Example 2.1: Classifying an Attack

An employee receives an email that appears to come from the bank's IT team asking her to log in on a link to "verify" her account. After she does, the attacker uses her credentials to access the company network. Identify the attack types.

Solution

The first stage is **phishing** (spear phishing if targeted at her), a form of **social engineering**. The second stage is **unauthorised access** using stolen credentials. Controls: user awareness training, multi-factor authentication, email filtering, and logging of unusual log-ins.

2.2 The CIA Security Triad

The **CIA triad** is the foundation model of information security. Every security control aims to protect one or more of its three goals.



Figure 2.1: The CIA security triad

Goal	Meaning	Threat example	Typical controls
Confidentiality	Only authorised people can view information.	Data breach, eavesdropping, shoulder surfing	Encryption, access control, authentication, classification
Integrity	Information stays accurate, complete and unaltered by unauthorised parties.	Tampering, malware, unauthorised edits	Hashing, digital signatures, version control, audit logs
Availability	Systems and data are accessible when needed.	DDoS, ransomware, hardware failure, power cuts	Backups, redundancy, DR plan, DDoS protection, patching

Note: Extended models add authenticity, non-repudiation (a sender cannot deny sending) and accountability. Balance is needed: too much confidentiality (strict locks) can reduce availability.

Implementing CIA at Four Levels

Level	Measures
Organisational	Risk assessment; written security policies; assigned responsibilities; security awareness training; least privilege and separation of duties; business continuity and disaster recovery plans; vendor management; regular audits (ISO/IEC 27001, NIST frameworks).
Network	Firewalls, intrusion detection/prevention systems (IDS/IPS), network segmentation and DMZ, VPN, TLS encryption, secure Wi-Fi, network access control, traffic monitoring.
Application	Secure coding (OWASP Top 10), input validation, authentication and session management, regular patching, code review, web application firewall, secure APIs.
End-user	Antivirus/EDR, automatic updates, strong passwords with MFA, disk encryption, regular backups, safe browsing, avoiding unknown attachments, reporting suspicious events.

2.3 Response to a Cyberattack

Prevention is never perfect, so every organisation needs an **incident response plan** and a trained **incident response team (CSIRT)**. The NIST model has four phases (Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-incident activity). The syllabus breaks the work into the steps below.

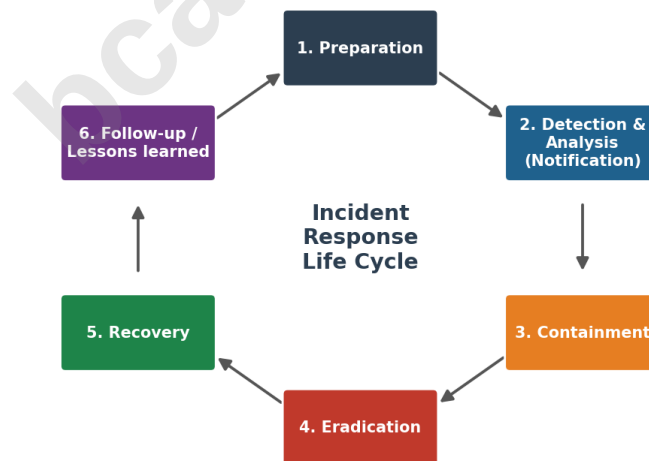


Figure 2.2: Incident response life cycle

1. Incident Notification

Once a suspected incident is detected, it must be reported quickly through a defined channel (help desk or security hotline). Key points: record who, what, when and how; notify the incident response team, management, and, as needed, legal counsel, affected customers, regulators, insurers and law enforcement. In Nepal, cybercrimes are reported to the **Cyber Bureau of Nepal Police**; the national CERT (NPCERT) also coordinates response. Avoid spreading rumours; share information on a need-to-know basis.

2. Protection of Evidence and Activity Logs

- Preserve logs (system, firewall, application, authentication) and make **secure copies**; protect them from alteration.
- Take forensic images of affected disks and memory **before** cleaning; record hash values (e.g., SHA-256) to prove the copy is unchanged.
- Maintain a **chain of custody**: a written record of who handled the evidence, when and why.
- Avoid actions that overwrite evidence (rebooting, running clean-up tools) until it is captured.

3. Incident Containment

Containment limits the damage and stops the spread. **Short-term**: disconnect infected machines, block malicious IP addresses, disable compromised accounts. **Long-term**: apply temporary fixes, move to clean systems, tighten access. The response must weigh business impact: shutting down a critical server has a cost, but letting an attack spread costs more.

4. Eradication

Remove the root cause: delete malware, close the exploited vulnerability by patching, reset all affected passwords and keys, rebuild compromised systems from trusted images, and confirm that backdoors are gone. Only then is **recovery** (restoring data from clean backups and returning systems to service under close monitoring) safe.

5. Incident Follow-Up

- Hold a **post-incident review** (lessons learned) and write an incident report.
- Estimate financial, legal and reputation damage; review if legal action is possible.
- Update policies, training and technical controls; improve detection.
- Decide whether to notify regulators or affected individuals as required by law or contract.

6. Using a Managed Security Service Provider (MSSP)

An **MSSP** is an external firm that monitors and manages an organisation's security (24×7 monitoring, firewall and IDS management, vulnerability scanning, incident response, compliance reporting).

Advantages	Disadvantages / risks
Round-the-clock expert monitoring	Loss of direct control; dependence on provider
Cheaper than building an in-house security operations centre	Provider may have access to sensitive data
Access to shared threat intelligence and tools	Slow response if service levels (SLAs) are weak
Frees staff for core business	Must still manage and audit the contract

7. Computer Forensics

Computer forensics is the collection, preservation, analysis and presentation of digital evidence in a way that is acceptable in court. It supports investigations of hacking, fraud, data theft, harassment and policy violations.

- **Identification** of possible sources of evidence (PCs, phones, servers, cloud, logs).
- **Preservation and collection:** forensic imaging using write-blockers; hash values; chain of custody. Collect volatile data (RAM, running processes, network connections) first, then disks.
- **Examination and analysis:** recover deleted files, examine timelines, e-mails, registry and browser history; search keywords.
- **Reporting and presentation:** clear, factual report; expert testimony if required.
- **Tools (examples):** Autopsy/The Sleuth Kit, FTK, EnCase, Volatility (memory), Wireshark (network).

Note: Investigators must work on a copy, never the original. Any break in the chain of custody can make evidence inadmissible.

2.4 Cyber Law

Cyber law (IT law) is the body of law governing activities in cyberspace: electronic records and signatures, e-commerce, cybercrime, privacy and data protection, intellectual property online, and jurisdiction. It is needed because traditional laws were written for the paper world and do not clearly cover digital evidence, online contracts and cross-border crime.

Main Areas of Cyber Law

- **Cybercrime:** hacking, malware, online fraud, identity theft, cyberstalking, illegal content.
- **Electronic transactions:** legal validity of e-contracts, e-records and digital signatures.
- **Data protection and privacy.**
- **Intellectual property online:** copyright, domain names, software piracy.
- **Jurisdiction and cross-border cooperation.**

Important International Instruments (for reference)

Instrument	Point
UNCITRAL Model Law on Electronic Commerce (1996)	Model for giving e-records the same legal status as paper; influenced many countries, including Nepal's ETA.
Budapest Convention on Cybercrime (2001)	First major international treaty on cybercrime and cross-border evidence sharing.
EU GDPR (in force May 2018)	Strong data-protection regime with heavy fines.
US CFAA (1986)	US federal law against unauthorised computer access.

2.5 Provisions of the Electronic Transactions Act, 2063 of Nepal

The **Electronic Transactions Act, 2063 BS** (often cited as 2006 or 2008 AD) is Nepal's main cyber law. It came after an ordinance (2061 BS) and follows the UNCITRAL model. Its purposes are to give legal recognition to electronic records and digital signatures, to make electronic transactions reliable, to regulate certifying authorities, and to define computer-related offences and penalties.

Main Contents

- **Legal recognition** of electronic records and digital signatures: where law requires a document or signature, an electronic record or digital signature that meets the Act's conditions is valid.
- **Dispatch, receipt and acknowledgement** of electronic records: rules on when a message is treated as sent or received.
- **Digital signatures and certificates:** the Act creates the **Controller of Certification** (under the ministry in charge of information and communication) who licenses **Certifying Authorities** that issue digital signature certificates, and states duties of subscribers.
- **Government use of electronic records** and digital signatures in official work.

- **Network service providers:** limits on liability for content merely carried, and duties to help investigations.
- **Computer-related offences and penalties** (Sections 44 onwards).
- **Information Technology Tribunal** to hear cases under the Act, with an Appellate Tribunal for appeals. Note: in practice cybercrime cases have been tried in district courts; check current practice.
- **Extra-territorial reach:** the Act can apply to offences committed outside Nepal if they involve a computer, system or network located in Nepal.

Key Offences and Penalties

Section	Offence	Maximum penalty (as reported)
44	Pirating, destroying or altering computer source code that the law requires to be kept	Up to 3 years' imprisonment, or fine up to Rs 2,00,000, or both
45	Unauthorised access to computer materials (hacking) or exceeding authorised access	Fine up to Rs 2,00,000, or up to 3 years' imprisonment, or both
46	Damage to a computer, program or information (destroying, deleting, altering, disrupting)	Up to 3 years' imprisonment and/or fine (sources report a very small fine, Rs 2,000, in the original text; verify)
47	Publishing or displaying illegal material in electronic form (content against public morality or decency, or that spreads hatred or jealousy between castes/communities)	Up to 5 years' imprisonment, or fine up to Rs 1,00,000, or both
Other	Breach of confidentiality, false statements or licences relating to digital signatures, computer fraud, abetment, attempt	Various; see the Act (e.g., computer fraud is commonly cited at up to 2 years and Rs 1,00,000)

Note: Section 47 is the most frequently used and most criticised provision. Critics say its wording is vague and has been used against journalists and social-media users, which raises freedom-of-expression concerns (see Unit 3). A new Information Technology / cyber-security bill has been proposed for years to replace or update the ETA; its current status should be checked.

Other Related Nepali Laws and Policies

- **Constitution of Nepal (2015):** right to privacy (Art. 28), freedom of expression (Art. 17).
- **Muluki Criminal Code, 2074 (2017):** covers forgery, defamation, fraud and offences that also occur online.
- **Individual Privacy Act, 2075 (2018):** protection of personal information.
- **National Cyber Security Policy (2023)** and **Digital Nepal Framework (2019):** policy direction for critical infrastructure protection and digital services.

- **Copyright Act, 2059** (2002): software and digital content (see Unit 4).

Example 2.2: Which Section Applies?

(a) A former employee logs in to his old company's server using an unclosed account and deletes files. (b) A person posts a defamatory and obscene video about a neighbour on Facebook.

Solution

(a) Unauthorised access (Section 45) and damage to information (Section 46) of the ETA. (b) Publishing illegal electronic material (Section 47); defamation and related provisions of the Muluki Criminal Code may also apply.

2.6 Important Short Questions (Exam Practice)

- Define computer incident. List and explain five types of exploits.
- Explain the CIA triad with examples. How can CIA be implemented at network and application level?
- Describe the steps of responding to a cyberattack.
- What is computer forensics? Why is chain of custody important?
- What are the advantages and disadvantages of using an MSSP?
- What is cyber law? Explain the main provisions of the ETA 2063 of Nepal.

Key Takeaways

- ✓ Threat + vulnerability = risk; exploits range from malware to social engineering.
- ✓ CIA (confidentiality, integrity, availability) drives all security controls; apply at organisation, network, application and user levels.
- ✓ Response: notify, protect evidence and logs, contain, eradicate, recover, follow up.
- ✓ Forensics needs preserved evidence, hashes and chain of custody.
- ✓ MSSPs give expertise and 24×7 monitoring but reduce control.
- ✓ Nepal's ETA 2063 recognises e-records and digital signatures and defines offences (Sections 44 to 47 are key).
- ✓ Section 47 (illegal content) is powerful but controversial.

— *End of Unit 2* —