Ethical and Professional issues in Information Security

Ethical Dilemma in Project Management

Alternative Dispute Resolution (ADR)

Hands-on cybersecurity tools

Case Study on Cyber Crime

Ethical Dilemma in Project Management

- An ethical dilemma occurs when a project manager or team faces a situation where there are conflicting values, responsibilities, or decisions — and no clear "right" answer.

- In project management, especially in information security, ethical dilemmas arise when doing what's legally correct may conflict with what is morally or professionally right, or when business goals challenge ethical behavior.

Common Ethical Dilemmas

- **Data Privacy vs. Business Interests:**
  Should you share customer data to benefit the company, even if the user hasn’t given consent?

- **Meeting Deadlines vs. Quality & Security:**
  Should you skip security testing to meet the project deadline?

- **Truth in Reporting Progress:**
  Is it okay to hide issues or bugs from clients to avoid blame or penalties?

- **Use of Surveillance Tools:**
  Is it ethical to monitor employees’ digital activities without their knowledge?

How to handle Ethical Dilemmas?

1. Follow Professional Codes of Conduct.

2. Apply Ethical Frameworks

   Utilitarian frame- decision makes the most benefit

   Rights-based- Does it respect the rights of all stakeholders

   Fairness/Justice- Is it fair to everyone involved

3. Consult with Stakeholders or Legal Counsel.

4. Document and Communicate Decisions Clearly.

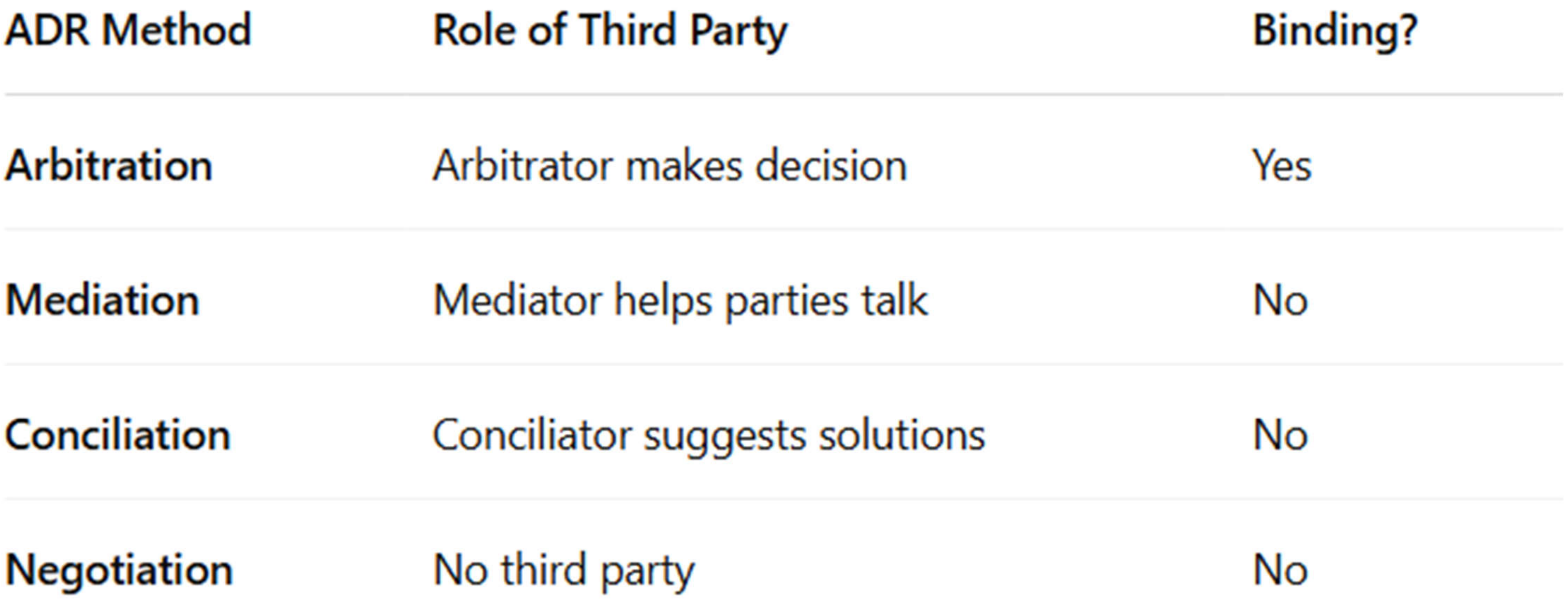
Alternative Dispute Resolution (ADR)

- Methods of resolving disputes outside of the traditional court system.

- It includes processes that are usually faster, less expensive, confidential, and less formal.

- Commonly used in business contracts, technology disputes, and information security issues.

Types of ADR



ADR Method	Role of Third Party	Binding?
Arbitration	Arbitrator makes decision	Yes
Mediation	Mediator helps parties talk	No
Conciliation	Conciliator suggests solutions	No
Negotiation	No third party	No

Hands-on cybersecurity tools

Using hands-on cybersecurity tools is a key part of defending digital systems.

From scanning networks to cracking passwords and analyzing malware.

These tools give professionals the **power to secure and safeguard information** in a practical, real-world environment.

Categories and Examples

1. Network Security Tools

Used to scan and monitor networks for vulnerabilities and intrusions.

- **Wireshark**: Network protocol analyzer to capture and analyze packets
- **Nmap**: Port scanner to discover hosts and services on a network
- **Snort**: Intrusion detection/prevention system (IDS/IPS)

2. Penetration Testing Tools

Simulate cyberattacks to identify weaknesses.

- **Kali Linux**: A Linux distro packed with hundreds of cybersecurity tools
- **Metasploit**: Framework for developing and executing exploit code
- **Burp Suite**: Web vulnerability scanner and testing tool

3. Password Cracking Tools

Used to test password strength or recover lost passwords.

- **John the Ripper**: Password cracker
- **Hashcat**: Advanced password recovery tool

4. Encryption Tools

Protect data using cryptographic methods.

- **VeraCrypt**: File encryption tool
- **GPG (GNU Privacy Guard)**: Secure communication and data storage

5. Antivirus & Malware Analysis Tools

Detect and remove malicious software.

- **Malwarebytes**: Malware detection and removal
- **VirusTotal**: Online scanner for files and URLs

6. Log Monitoring & SIEM Tools

Analyze security events and logs.

- **Splunk**: Searches, monitors, and analyzes machine data
- **ELK Stack** (Elasticsearch, Logstash, Kibana): For log analysis and visualization

Case Study on Cyber Crime