CSE332
INDUSTRY ETHICS AND LEGAL ISSUES

Ethical and Professional issues in Information Security

Law and Ethics in Information Security

- Laws: Rules adopted and enforced by governments to codify expected behavior in modern society

- Ethics: Relatively fixed moral attitudes or customs of a societal group (based on cultural mores)

- The key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not

Law and Ethics in Information Security

- Law and ethics guide cybersecurity practices.
- Laws ensure data protection and privacy.
- Ethics focus on responsible security decisions.
- Cyber laws prevent hacking and misuse.
- Privacy rights balance security and access.
- Compliance ensures trust and legal safety.

Features of Law and Ethics in Information Security

- **Data Protection** – Ensures confidentiality and integrity of information.
- **Privacy Regulations** – Safeguards personal and sensitive user data.
- **Cybercrime Prevention** – Criminalizes hacking, fraud, and cyber threats.
- **Compliance Standards** – Organizations must follow legal frameworks.
- **Intellectual Property Protection** – Secures software, patents, and copyrights.
- **Accountability** – Holds individuals and organizations responsible.

Types of Laws in Information Security

- **Data Protection Laws** – Regulate data collection, storage, and processing. *(e.g., GDPR, CCPA, HIPAA)*
  - GDPR(General Data Protection Regulation) – European law that gives individuals control over their personal data.
  - CCPA (California Consumer Privacy Act) – Protects the privacy rights of consumers in California.
  - HIPAA (Health Insurance Portability and Accountability Act) – Protects medical information in the U.S.
- **Cybercrime Laws** – Prevent hacking, fraud, and identity theft. *(e.g., CFAA, UK Computer Misuse Act)*

  CFAA(Computer Fraud and Abuse Act) – U.S. law that criminalizes unauthorized access to computers

  UK Computer Misuse Act – UK legislation targeting cyberattacks and unauthorized system access.
- **Intellectual Property Laws** – Protect software, trademarks, and copyrights. *(e.g., Copyright Act, Patent Laws)*

Types of Laws in Information Security

- **Compliance and Regulatory Laws** – Ensure businesses follow security standards. *(e.g., ISO 27001, PCI DSS)*

  ISO **27001** – International standard for information security management

  PCI DSS (Payment Card Industry Data Security Standard) – Ensures secure handling of credit card data.

- **Surveillance and Privacy Laws** – Balance national security with individual privacy. *(e.g., FISA, ECPA)*

  FISA (Foreign Intelligence Surveillance Act), CPA (Electronic Communications Privacy Act)

- **Contract and Liability Laws** – Govern security obligations in business agreements. *(e.g., NDA in cybersecurity contracts)*

Types of Ethics in Information Security

- **Privacy Ethics** – Ensures responsible handling of user data.
- **Hacking Ethics** – Differentiates ethical hacking (white-hat) from malicious hacking (black-hat).
- **AI and Security Ethics** – Manages bias, transparency, and accountability in security AI.
- **Corporate Ethics** – Defines security responsibilities of organizations.
- **Whistleblowing Ethics** – Protects individuals reporting security violations.
- **Cybersecurity Professional Ethics** – Guides IT professionals on ethical security practices.

Examples of Law and Ethics in Information Security

- Facebook-Cambridge Analytica Scandal (Privacy Ethics & Data Protection Laws Violation)
- WannaCry Ransomware Attack (Cybercrime & Compliance Failure)
- Apple vs. FBI Encryption Case (Privacy vs. Surveillance Ethics)
- Google AI Bias in Hiring (AI and Security Ethics Concern)
- Edward Snowden NSA Leaks (Whistleblowing & Government Surveillance Ethics)
- Sony Pictures Hack (Intellectual Property & Cybercrime Violation)

Advantages and Disadvantages of Law and Ethics in Information Security

Advantages:

- **Data Protection** – Ensures confidentiality and prevents unauthorized access.
- **Privacy Assurance** – Strengthens user trust in organizations.
- **Cybercrime Prevention** – Reduces risks of hacking and fraud.
- **Legal Compliance** – Avoids lawsuits and regulatory penalties.
- **Corporate Accountability** – Holds businesses responsible for security breaches.
- **Ethical Decision-Making** – Encourages responsible cybersecurity practices.

Disadvantages:

- **Compliance Costs** – Implementing security laws can be expensive.
- **Restrictive Policies** – May limit innovation and data access.
- **Legal Complexity** – Varying global regulations make compliance challenging.
- **Slow Legal Updates** – Laws may not keep speed with new cyber threats.

Organizational Liability and the Need for Counsel

- Organizations are legally and ethically responsible for protecting the data they collect, store, and process. This includes customer data, employee records, intellectual property, and any sensitive business information.
- Failure to comply with security laws and ethical standards can result in legal penalties, financial losses, and reputational damage.

Organizational Liability in Information Security

Organizations can be held liable or legally responsible for:

- **Data Breaches** – If a company fails to protect personal data (like customer or employee info) and it gets stolen or leaked.
- **Non-Compliance with Regulations** – Violating legal rules or laws can result in heavy fines.
- **Cybersecurity Negligence** – Failure to implement security measures can lead to legal action.
- **Intellectual Property Violations** – Unauthorized use of copyrighted or patented technology.
- **Insider Threats and Employee Misconduct** – Misuse of company data by employees leading to legal liability.

Need for Legal Counsel in Cybersecurity

Organizations require legal counsel to:

- **Ensure Compliance** – Guide businesses on adhering to global cybersecurity regulations.
- **Manage Data Protection Policies** – Develop legal policies for handling customer and employee data.
- **Handle Cybersecurity Incidents** – Provide legal defense in case of breaches or cyberattacks.
- **Draft Contracts and Agreements** – Ensure secure and legally binding terms in business deals.
- **Risk Assessment and Mitigation** – Identify potential legal risks and prevent liabilities.

Examples of Organizational Ethics and Liability in Information Security

- Facebook-Cambridge Analytical Scandal (Ethical and Legal Violations in Data Privacy)
- Equifax Data Breach (Failure to Ensure Ethical Cybersecurity Practices)
- Uber Data Breach Cover-Up (Lack of Transparency and Ethical Conduct)
- Wells Fargo Fake Accounts Scandal (Unethical Employee Behavior and Corporate Accountability)
- Yahoo Data Breach (Corporate Negligence in Cybersecurity and Legal Repercussions)

Answer the following questions

- What happens without ethical employee conduct?
- How does unethical behavior harm organizations?
- What legal risks arise from misconduct?
- Why is customer trust easily lost?
- Can organizations face penalties for employees?
- How does non-compliance affect reputation?

Policy Versus Law

1. Definition

- **Policy** – An internal rule or guideline **created by an organization** to guide employee behavior and decision-making.
- **Law** – An official rule **created by the government** that applies to everyone in a country or state.

2. Purpose

- **Policy** – Ensures consistency, security, and ethical conduct within an organization.
- **Law** – Maintains order, protects rights, and enforces justice in society.

3. Enforcement

- **Policy** – Enforced internally by management or HR departments.
- **Law** – Enforced by government authorities and courts.

4. Consequences of Violation

- **Policy** – Can lead to warnings, termination, or internal penalties.
- **Law** – Can result in legal action, fines.

5. Flexibility

- **Policy** – Can be modified by the organization as needed.
- **Law** – Requires legal procedures or approval to change.

6. Scope

- **Policy** – Applies only within an organization or institution.
- **Law** – Applies to everyone within a country or state.

Policies in Information Security

- **Acceptable Use Policy (AUP)** – Defines proper use of company systems and networks.
- **Password Management Policy** – Sets rules for creating and maintaining secure passwords.
- **Data Backup and Recovery Policy** – Outlines procedures for data protection and restoration.
- **Incident Response Policy** – Establishes steps to follow during cybersecurity incidents.
- **Access Control Policy** – Determines user roles and permissions for system access.

Laws in Information Security

- **General Data Protection Regulation (GDPR)** – Protects personal data of EU citizens.
- **Health Insurance Portability and Accountability Act (HIPAA)** – Ensures security of healthcare information.
- **Computer Fraud and Abuse Act (CFAA)** – Criminalizes unauthorized computer access.
- **Cybersecurity Information Sharing Act (CISA)** – Encourages data sharing for cybersecurity.
- **Digital Millennium Copyright Act (DMCA)** – Protects digital content and intellectual property.
- **California Consumer Privacy Act (CCPA)** – Regulates data privacy rights for California residents.

Differences Between Policy and Law

Criteria	Policy	Law
Nature	Internal organizational rule	Government-enforced legal rule
Objective	Guides employees’ actions and decisions	Maintains societal order and justice
Authority	Created by an organization	Created by legal bodies
Applicability	Limited to a specific organization	Applies to all individuals and entities
Modification	Can be updated internally as needed	Requires a legal process to change
Enforcement	Managed by HR or internal teams	Enforced by courts and legal agencies
Consequences	Can result in warnings or termination	Can lead to fines, penalties, or jail
Example	Company cybersecurity policy	Data privacy law (e.g., GDPR, HIPAA)