

Class Exercise: Legal, Ethical, and Professional Issues in Information Security

Objective: Understand and analyse the legal, ethical, and professional issues in information security by examining real-world scenarios and applying relevant principles and laws.

Instructions:

1. Form groups of 3-4 students.
2. Each group will be assigned a scenario related to information security.
3. Discuss the scenario within your group and answer the questions provided.
4. Submit your findings to the topic forum on Moodle.
5. Present your findings to the class.

Scenario 1: Data Breach at a Financial Institution

Scenario: A major financial institution experiences a data breach that compromises the personal and financial information of millions of customers. The breach was caused by a failure to update security software, despite multiple warnings from the IT department.

Questions:

1. **Legal Issues:**
 - Identify the laws and regulations that apply to this scenario?
 - What are the potential legal consequences for the financial institution?
2. **Ethical Issues:**
 - What ethical responsibilities does the financial institution have towards its customers?
 - How should the company address the breach ethically?
3. **Professional Issues:**
 - What professional standards and practices were neglected?
 - How can the institution improve its information security practices preventing future breaches?

Scenario 2: Insider Threat in a Healthcare Organization

Scenario: An employee at a healthcare organization intentionally accesses and sells patient records to a third party. The employee bypassed security protocols to obtain this information.

Questions:

1. **Legal Issues:**
 - What laws protect patient?
 - What legal actions can be taken against the employee and the organization?
2. **Ethical Issues:**
 - Discuss the ethical implications of the employee's actions.
 - What ethical considerations should guide the organization's response to the breach?
3. **Professional Issues:**

- Identify the professional obligations of employees in handling sensitive information.
- What measures can the organization implement to detect and prevent insider threats?

Scenario 3: Intellectual Property Theft at a Tech Company

Scenario: A former employee of a tech company steals proprietary software code and uses it to start a competing business. The employee argues that they significantly contributed to the development of the software.

Questions:

1. **Legal Issues:**
 - What intellectual property laws are relevant to this?
 - How can the tech company legally protect its intellectual property?
2. **Ethical Issues:**
 - Was it ethical for the employee to use the proprietary code for personal gain? Why or why not?
 - What ethical principles should guide the tech company's response?
3. **Professional Issues:**
 - What professional standards apply to the handling of proprietary information?
 - How can the tech company strengthen its policies to protect intellectual property?

Scenario 4: Social Media Privacy Concerns

Scenario: A social media company collects extensive user data without clear consent and shares it with third-party advertisers. Users are unaware of the extent of data collection and its use.

Questions:

1. **Legal Issues:**
 - Which privacy laws are potentially violated in this ?
 - What legal recourse do users have against the social media company?
2. **Ethical Issues:**
 - Evaluate the ethicality of the social media company's data collection practices.
 - How should the company address user privacy concerns ethically?
3. **Professional Issues:**
 - What professional standards should guide the company's data handling practices?
 - What changes can the company make to ensure transparency and user trust?