# Case Study 1

Financial Services Corp, a prominent financial institution, experienced a severe security breach when Tom, a disgruntled IT employee, used his administrative access to steal sensitive customer information, including bank account details and personal identification numbers. Tom intended to sell this data on the dark web to retaliate against the company for perceived grievances. The breach was detected when unusual account activities were reported by multiple customers, leading to an internal investigation. Financial Services Corp reported the incident to the authorities, and Tom was arrested and charged under the Computer Misuse Act 1990.

**Analytical Questions**

1) What specific sections of the Computer Misuse Act 1990 did Tom violate, and why are these sections applicable?

ANS:

Tom violated Section 1 (unauthorized access to computer material) and Section 3 (unauthorized modification of computer material). Section 1 is applicable because Tom accessed customer data without legitimate authorization. Section 3 applies because he altered the integrity of the data by copying and attempting to sell it, which constitutes unauthorized modification.

2) How did Tom’s position as an IT employee facilitate his criminal activities, and what does this imply about insider threats?

ANS:

Tom’s IT position gave him elevated access privileges, which he exploited to access and steal sensitive data. This implies that insider threats are particularly dangerous because employees with legitimate access can misuse their privileges. It highlights the necessity for strict access controls and monitoring systems to detect and prevent unauthorized activities by insiders.

3) What were the immediate and long-term consequences for Financial Services Corp following the data breach?

ANS:

Immediately, Financial Services Corp faced customer distrust, potential lawsuits, and regulatory scrutiny. The company had to invest heavily in cybersecurity improvements and customer compensation. Long-term consequences included reputational damage, loss of business, and ongoing legal and regulatory challenges. The breach underscored the importance of robust cybersecurity practices and crisis management strategies.

4) What legal penalties could Tom face under the Computer Misuse Act 1990, and how do these penalties serve as a deterrent?

ANS:

Tom could face up to five years in prison and/or a substantial fine under Section 3 of the Computer Misuse Act 1990. These penalties serve as a deterrent by highlighting the serious consequences of cybercrimes, thus discouraging individuals from engaging in unauthorized access and data theft. The severe penalties aim to protect the integrity of computer systems and data.

5) How could Financial Services Corp have better protected their sensitive customer information from internal threats?

ANS:

Financial Services Corp could have implemented stricter access controls, regularly audited employee activities, and used advanced encryption for sensitive data. Employing multi-factor authentication, conducting background checks on employees, and establishing a whistleblowing system for reporting suspicious behavior would also enhance security. These measures would help detect and mitigate insider threats more effectively.

# Case Study 2

KidZone Games, a popular online gaming platform for children, came under scrutiny when it was discovered that the company had been collecting personal information from users under the age of 13 without obtaining verifiable parental consent. The data collected included names, email addresses, and geolocation information. Additionally, KidZone Games used this data to target children with personalized advertisements. The Federal Trade Commission (FTC) launched an investigation, which revealed that KidZone Games was in violation of the Children’s Online Privacy Protection Act (COPPA). As a result, the company faced substantial fines and was required to implement comprehensive privacy measures to protect young users.

**Analytical Questions**

1) What specific requirements of the Children’s Online Privacy Protection Act (COPPA) did KidZone Games violate, and why are these requirements important?

ANS:

KidZone Games violated COPPA by collecting personal information from children under 13 without obtaining verifiable parental consent. These requirements are important because they protect children’s privacy and safety online, ensuring that their data is not collected or used in ways that could harm them or expose them to inappropriate content.

2) How did the FTC determine that KidZone Games was in violation of COPPA, and what evidence was crucial in this determination?

ANS:

The FTC determined the violation through an investigation that included examining the company’s data collection practices and reviewing complaints from parents and watchdog groups. Crucial evidence included logs of data collected without consent, records of targeted advertisements to children, and the absence of parental consent forms.

3) What were the immediate and long-term consequences for KidZone Games following the FTC’s findings?

ANS:

Immediately, KidZone Games faced substantial fines and negative publicity. Long-term consequences included implementing comprehensive privacy measures, undergoing regular compliance audits, and rebuilding trust with users and parents. The company also had to invest in training and new technology to ensure ongoing COPPA compliance, impacting their operational costs.

4) What steps should KidZone Games have taken to comply with COPPA from the outset?

ANS:

KidZone Games should have implemented a system to obtain verifiable parental consent before collecting personal information from children. This includes clear privacy policies, mechanisms for parents to review and delete their children’s information, and age verification processes. Regular audits and compliance checks should have been established to ensure adherence to COPPA regulations.

5) How can online platforms balance user engagement and compliance with child privacy laws like COPPA?

ANS:

Online platforms can balance engagement and compliance by designing engaging, age-appropriate content that does not require personal data collection. If data collection is necessary, they should ensure robust consent processes, transparent privacy practices, and tools for parents to manage their children’s data. Regularly updating these practices based on regulatory changes and technological advancements is also essential.

6) What role do parents play in ensuring their children’s online privacy, and how can companies facilitate this role?

ANS:

Parents play a crucial role by monitoring their children’s online activities and understanding the privacy policies of the platforms they use. Companies can facilitate this by providing clear, accessible information about data practices, offering parental controls, and creating easy-to-use mechanisms for obtaining and managing consent. Education initiatives to inform parents about online privacy risks and protections are also beneficial.

# Case Study 3

Consider the following case study, and answer the two questions in 50 words each. Dr. Emily, a dedicated data scientist, is leading the development of an AI-driven diagnostic tool for a new healthcare company. This innovative tool exhibits remarkable potential to significantly enhance diagnostic precision through medical imaging. During rigorous testing, however, Dr. Emily discovers a critical concern – it occasionally generates false positives, potentially leading to erroneous diagnoses. Pressured by the company's leadership, driven by the desire for a quick market entry, Dr. Emily faces an ethical dilemma – launch the tool as it is, potentially endangering patients, or insist on rectifying the issue before deployment.

As Dr. Emily struggles with this ethical dilemma, she finds herself at the intersection of patient safety, transparency, and medical accuracy – all integral aspects highlighted by the ACM Code of Ethics and Professional Conduct. Her primary concern is to ensure that the AI tool's outputs are dependable and that the well-being of patients takes priority over profit-driven motives. In navigating this complex situation, Dr. Emily must maintain a delicate balance between adhering to ethical principles and aligning with her employer's aspirations for swift market entry, all while safeguarding patient welfare.

**Analytical Questions**

a) Discuss how Dr. Emily can address the pressure from the company’s leadership.

ANS:

Dr. Emily can advocate for patient safety by presenting evidence of the tool’s false positives and their potential harm. She should reference the ACM Code of Ethics, propose a timeline for addressing issues, and emphasize long-term trustworthiness and regulatory compliance as essential for the company's reputation and success.

b) Advise on how the company can avoid such ethical dilemmas in the future when developing AI healthcare tools.

ANS:

The company should implement a rigorous ethical framework for AI development, prioritize extensive testing, and establish a cross-functional ethics committee. Incorporating patient safety as a core value, aligning goals with regulatory standards, and promoting a transparent culture can prevent profit-driven compromises and ensure trustworthy healthcare tools.