5.3: Data Ethics: Security & Privacy

Scenario 1: Your role at Pig E. Bank is to develop models that detect suspicious account activity associated with money laundering. Your current project requires you to distribute prototype model outputs to your team of investigators for validation. Standard investigation procedure requires the investigator to access client PII and account information to build a customer profile before dispositioning the model output. One day, you notice one of your investigators taking a photo of his screen while sensitive client data is displayed.

A. Is this a data privacy issue, data security issue, or both? Please provide a short explanation for your answer.

   This situation raises concerns regarding the security and privacy of data. The protection and proper handling of client personally identifiable information (PII) is crucial, and it should be stored and managed by relevant laws and established procedures. The act of capturing a photo of PII using a mobile phone and storing it on an employee's device violates these policies and gives rise to security concerns. The investigator is required to comply with Pig E. Bank's standards for handling and storing personal data as a condition of their employment. There are more secure methods available for data collection, making the investigator's use of an unauthorized and unprotected approach unjustified. Client PII should only be accessed through secure and authorized platforms, and the investigator's equipment is unlikely to meet those criteria.

B. What would be the risks to Pig E. Bank and its customers if this issue weren't addressed?

   A security breach involving the client's PII could endanger Pig E. Bank and potentially lead to legal consequences. This incident has the potential to facilitate identity theft and fraudulent activities. Sharing or utilizing consumer information for purposes unrelated to the project would constitute a security breach. If the client's PII and account information are leaked, both Pig E. Bank and its clients may face adverse legal and financial consequences. Regardless of the employee's intentions, the act of taking a photo violates data privacy laws internally and externally, significantly increasing the risk of a security breach. Failure to address this issue exposes Pig E. Bank and its customers to potential monetary and legal ramifications.

C. To prevent this type of data theft in the future, what changes would need to be made to the policies around data access?

   The investigator should be investigated and terminated immediately due to their lack of experience and involvement in a money laundering investigation. Pig E. Bank should implement comprehensive background checks for all personnel and conduct regular training sessions on data protection and security. It is crucial to address the investigator's case as a means of informing staff members about the consequences of violating data privacy policies. Access to the customer's PII and account details should be limited, and guidelines should align with the basic requirements of Health Insurance Portability and Accountability Act (HIPAA). Employees handling PII should

undergo advanced training and face appropriate consequences. To enhance protection, anonymizing or encrypting the dataset may be necessary.

Scenario 2: Your manager has asked you to join them in representing the compliance analytics department at the compliance committee meeting. At the meeting, the prospect of outsourcing some lower-level analytical functions to a contractor in a foreign country is discussed, and it appears to be popular with the other department heads. Outsourcing could save the bank millions of dollars per year in labour costs, and the department heads seem confident that this won't violate data privacy laws. You know from experience that some of your bank's customers can be identified as being on active military duty and, like all clients, you keep records of their pay grade, address, contact information, and other PII.

A. Does this scenario highlight a data privacy issue, data security issue, or some other ethical issue? Explain your answer.

   The outsourcing of data to a foreign jurisdiction raises concerns regarding data privacy, security, and transparency. Pig E. Bank must ensure the protection of client information while also adhering to security guidelines and international laws. There is a risk that customers may not be aware of potential data breaches, particularly for service members, which raises concerns about transparency. Moreover, by granting access to data in regions lacking similar privacy regulations as the United States, Pig E. Bank may be in violation of their data security program. Unauthorized access, use, and transfer of consumer identifiers could occur without proper notification. Outsourcing analytics results in reduced control and oversight over data processing, thereby posing risks to both data privacy and security.

B. How would you communicate your concerns to the compliance committee? To answer this question, you can rely on either your previous work experience or the tips provided in the Exercise, but be as specific as you can.

   While outsourcing offers certain benefits, it also brings about increased risks and expenses. Conducting thorough research on privacy regulations is crucial, and implementing strong internal data protection measures is essential to safeguard both the company's reputation and the sensitive information of its clients. Effective communication can be achieved by addressing concerns, providing clarifications, and answering questions. While cost-cutting measures may be considered, they should not jeopardize data security or increase the risk of data breaches. It is important to provide specific recommendations that outline steps for protecting the privacy of PII.

   To facilitate the compliance committee's evaluation, preparing a presentation or package on data privacy, security, and ethical issues would be beneficial. Additionally, addressing labour costs can be achieved by focusing on process improvement and productivity rather than solely relying on outsourcing. By emphasizing these aspects, the same goals can be accomplished while minimizing risks and maintaining data security.

C. If Pig E. Bank does go ahead and outsource some of its analytical functions, how would you anonymize the data while ensuring that someone can still conduct an analysis?

Data anonymity can be achieved through encryption, limiting access to authorized personnel, or removing PII before sharing it with overseas contractors. Certain analytical functions may not require any PII from contractors to be performed effectively. Employing differential privacy techniques can enhance data anonymization, but it may impact the usefulness of analysis results for commercial decision-making. While encryption and removing client identification can potentially anonymize data, there is still a risk to data security. In such cases, sensitive data should be completely deleted from transmitted data, and any remaining information should be cleansed to eliminate any PII.

Scenario 3: Let's suppose you've lived and worked in different cities around the world, and you're interested in learning more about how other countries have dealt with data ethics.

A. Research a case study from your own country where a company or organization has acted unethically in terms of collecting and sharing data. You're free to use information you find on the internet, but make sure you include the link to your resources in your document.

In 2018, British Airways suffered a data breach that affected 380,000 transactions made via its website and mobile app. Unauthorised access was acquired to consumer data, including personal and financial information. The hack sparked worries about British Airways' security safeguards and customer data processing (BBC NEWS, 2020, Wikipedia, 2020).

B. Explain what the company or organization did exactly. Did they act according to regional or national laws?

Following the 2018 data breach, British Airways was the subject of an investigation by the Information Commissioner's Office (ICO), the data protection authority, as it is governed by regional and national regulations in the UK. British Airways' adherence to the General Data Protection Regulation (GDPR), which was adopted into UK legislation, was evaluated by the ICO. The investigation found that the business had violated GDPR rules by not taking adequate security measures.

C. Why was the company's behaviour unethical? (To answer this question, you can refer to this Exercise and the previous Exercise on data bias.)

For a number of reasons, British Airways' actions during the data leak can be viewed as immoral. They neglected their duty to secure customer information and did not put in place sufficient data security measures, allowing unauthorised access to client data. In addition, there was a delay in discovering and disclosing the breach, which made it difficult for those who were impacted to take the proper steps. The incident's aftermath saw insufficient customer communication, which made the company's unethical behaviour worse. Additionally, it was discovered that the business may not have complied with data protection rules, violating customers' rights to privacy. These

elements show a breach of the ethical standards that are expected of organisations that handle personal data.

D. What could you and the company have done to prevent this unethical behaviour? Please provide some concrete suggestions.

The business and its stakeholders had the opportunity to take many proactive measures to stop unethical behaviour like the British Airways data leak. This includes improving employee data protection training, implementing stringent access controls and encryption for sensitive data, making sure that systems and software are updated on a regular basis, creating an incident response plan, and promoting a culture of data privacy and ethical behaviour within the organisation. By putting these steps in place, businesses may actively endeavour to stop unethical behaviour, improve data security, and protect client privacy.

References:

1. Tidy, Joe (2020) *'British Airways fined £20m over data breach'* https://www.bbc.co.uk/news/technology-54568784
2. *Wiki (2020)'British Airways data breach'* https://en.wikipedia.org/wiki/British_Airways_data_breach