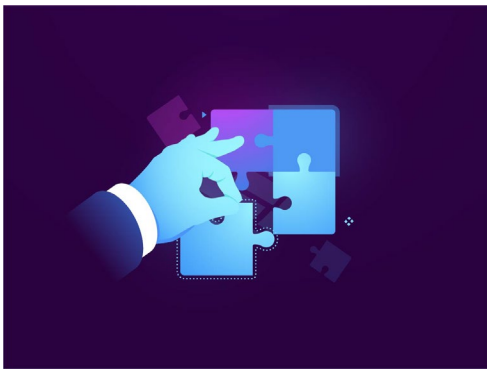
Southern New Hampshire University

DAT 250 Project Two: Riddle Security Scenario



Riddle Security is a 20-year-old company with a physical location in the United States. They are a third-party vendor that collects and stores information for companies in the United States and Canada. Riddle Security provides data backup and server infrastructure for companies that do not have adequate hardware for their needs. They are also able to access client (company) sales databases in order to collect and maintain customer information. This information consists of names, dates of birth, email addresses, phone numbers, partial social security numbers, and computer shopping preferences.

Riddle Security has an additional business in which the company collects data by monitoring online activity through social media and marketing companies. Riddle Security uses this data to build individual consumer profiles and categorizes those profiles into lists. These lists are made available on the open market for sale to advertisers.

Riddle Security maintains the data storage business and the consumer profiling data business in separate business categories. These two categories are not mixed; separate client revenue streams pay for their services and privacy concerns. The volume of data currently being housed consists of 250,000 individuals collectively.

Riddle has a policy to perform periodic compliance audits every three months. The compliance auditor, an employee of Riddle Security, falsified documents to show that there were periodic audits completed. The audits were not performed on schedule for a period of three cycles (nine months). The compliance auditor was also observed violating Riddle Security's policy of bringing external storage devices into secured areas.

The audit supervisor examined the records and learned that the audits had not been performed. She ordered a new audit to be performed ASAP. When the audit was completed, it was determined that there was a data breach from an outside entity seven months earlier. The breach could have been detected within weeks of it occurring had the audits happened on schedule.

Instead, the breach was open and ongoing for seven months and exposed client information for what appeared to be as many as 125,000 of the client accounts. There is no written practice based on industry standards as to how Riddle Security should respond from a legal or technical standpoint in response to this discovery.

The audit supervisor realized that this information must be reported, and decided to meet directly with the CEO of the company. The CEO wants a proposal on steps to implement a security breach protocol. The CEO is undecided as to whether or not a public notice should be given about the breach and asked for advice in this area.