**Class Activity**

**Name: Saman Khan**

**ID: 19K-0354**

**Section: H**

**Question#01: Explain the issue discussed in the article.**

The article "Boss I suspect someone has stolen the data" addresses the problem of how to react when there has been a breach of data. It explains the procedures that should be done to guarantee the data belonging to the firm is secure as well as how to respond to the event that has occurred. It discusses things like determining the extent of the harm, informing the appropriate authorities, and taking measures to prevent such occurrences in the future. In addition to this, it offers guidance on how to deal with the aftermath of a data breach, including how to communicate with consumers and how to restore trust in the firm.

**Question#02: What are the the existing preventive measures at the company and the relative standard compliance issues?**

The following are some preventative steps that businesses can take to safeguard their data, as outlined in the article:

* Implementing stringent authentication mechanisms
* Encrypting data
* Keeping an eye out for suspicious activities etc.

The importance of adhering to industry standards like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation is another topic that is covered in the article (GDPR). A company's level of compliance with these standards is one way to help verify that it is taking all of the essential precautions to protect its data.

**Question#03: Discuss the commentary made by the experts at the end and how can companies avoid the breach of data?**

At the very conclusion of the article, many industry professionals weigh in on the significance of being prepared with a strategy to deal with a data breach. They encourage businesses to establish a clear policy on how to respond to a breach and to ensure that all workers are aware of the policy. They also recommend that enterprises ensure that all employees are aware of the policy. In addition to this, they recommend that businesses keep a close eye on the state of their security protocols and modify them as necessary. Implementing stringent authentication procedures, encrypting data, and keeping an eye out for unusual activities are all other ways in which businesses can prevent data breaches.