DS-650 Assignment 2

What a breach means in terms of data: breaches mean anyone trying to steal or collect sensitive data from the system without the authorization of the system's owner. Sensitive data like Credit Card numbers, SSN numbers, Property Information, Bank Account Details, etc.

● Hacking or malware	25.0%
● Portable device loss	24.0%
● Unintended disclosure	17.4%
● Insider leak	12.0%
● Physical loss	11.6%
● Stationary device loss	5.4%
● Payment card fraud	1.4%
● Unknown	3.2%

Breach methods observed across industries

"There is some analysis from Google analysis was recorded between 2005 and April 2015"

Most of the breaches happened because of hacking or malware.

Some of them are happening because of insider leaks, payment card fraud, loss or theft, etc.

Sometimes attackers use social engineering tactics to collect data. They send malicious craft emails to persons to collect information through that email.

For example, the person got an email that her order is on hold because of the payment. Please click on the link the complete the payment. And user adds their details on that as they got the user's credit card or debit card details.

Types of data breaches are Compromised Credentials, Malware attacks, Ransomware attacks, Phishing, keyloggers, etc.

To avoid data breaches in any enterprise they have to make sure that all systems in the network are updated to prevent attackers from exploiting a vulnerability or any outdated software.

Keep employees updated about threats, and train them to watch out for social engineering.

Create a process to identify threats and vulnerabilities in networks. Perform security audits regularly and make sure all the systems in a network are accounted for.

They have to secure all the devices adding restrictions for the external storage devices.

Employees do not open any email that is not familiar to them or any unknown email from of domain network.

Rather than thinking breaches never going to happen, batter to mitigate as much risk as possible by taking some initial steps like two-step verification on account, and securing data by giving proper authentication.

Sometimes data breaches delete all your data. it's important to have a backup of your data so, that it can easily be recovered in case of data loss.

While changing any system make sure that before throwing out or selling destroy everything from the system.

Add some antivirus software to the system to protect against malware or any other virus that harms your device. Or do not open any link from your email or message from an unknown sender. Run antivirus before copying anything from the external hard drive or flash drive.

If you sending ant confidential data by email make sure that it open by the right person by encryption.

If you using a portable device like a flash drive, external hard drive, Phone, or Tablet make sure that the device is password protected or encrypted.

Take help of expert if you starting any business.

Reference :

1. https://www.google.com/search?q=what+is+data+breach%3F&rlz=1C1CHB F_enIN946IN946&oq=what+is+data+breach%3F&aqs=chrome..69i57j0i512l 9.10150j0j7&sourceid=chrome&ie=UTF-8
2. https://www.trendmicro.com/vinfo/us/security/definition/data-breach
3. https://www.sailpoint.com/identity-library/data-breach/?campaignid=11540240355&utm_source=google&utm_medium=cpc &utm_content=ams-bofu-all&ppgid=8416bb2f&cb={CACHEBUSTER}&gclid=CjwKCAjwp9qZBhBkEiwAs YFsb87v4d7f2yZiN79WKTON6WH4O4GuJzI8r4yE15yx54xQsb7Dg0DQqRoCBe YQAvD_BwE