SOME SECURITY STRATEGIES WHICH CAN MITIGATE DATA BREACH

To prevent and mitigate the impact of data breaches such as the recent one experienced by Latitude Financial, implementing an identity security program and implementing best practices is essential.

A comprehensive identity security program would include measures such as multi-factor authentication, privileged access management, and regular access reviews. These measures ensure that only authorized users have access to sensitive data, and their actions are limited within the system.

Multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of identification to access sensitive information. This ensures that even if one layer of security is compromised, there are additional safeguards in place.

Privileged access management ensures that only a limited number of users have access to sensitive data, and their permissions are closely monitored and controlled. This prevents unauthorized access and reduces the risk of insider threats.

Regular access reviews ensure that only authorized users have access to sensitive data, and permissions are regularly reviewed and updated. This ensures that access to sensitive information is always up-to-date and complies with data privacy regulations.

Implementing these measures is not enough. Continuous monitoring and analysis of user activity is crucial to detecting any abnormal or suspicious behavior, allowing quick action to prevent a data breach.

Let's quickly rush back to the IAM lifecycle we have

Access Management
Provisioning
Authentication (includes MFA, Multi layer controls)
Authorization (OAuth 2.0)

Self Services(Training required here on how customers make choice of password teach them how to choose password and when to change password, create a reminder).

Password management (get a good password manager, don't use same passwords in all your accounts).

Governance.(Do you have a good privacy policy between the third party, customer and resources owners?)

De-provisioning.
Do you have the Ability to disable, review, remove and delete unwanted privileged access accounts?
Don’t just disable and remove make sure you also delete that access from egress privileged access account.

This is just like a pendulum ball going thru and fro. You don't skip one step or Implement one or two and leave the rest.

Embrace Identity security program and Practices today to mitigate risk and data breaches within the organization.

Also Let's take a look at this PAM lifecycle Management which could also help mitigate this risk of cyber threat.

Define

Start by defining what 'privileged access' means and identify what a privileged account is for your organization. It's different for every company so it's crucial you map out what important business functions rely on data, systems and access. Gain a working understanding of who has privileged account access, and when those accounts are used.

Discover

Identify human and non-human privileged accounts and implement continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This helps ensure full, ongoing visibility of your privileged account landscape crucial to combating cyber security threats.

Manage and Protect

Proactively manage and control privileged account access, schedule password rotation, audit, analyze, and manage privileged session activity. For IT administrator privileged account users, you should control access and implement superuser privilege management to prevent attackers from running malicious applications, remote access tools, and commands. To prevent service account sprawl, implement proactive service account governance. Least privilege and application control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.

Monitor

Monitor and record privileged account activity. This will help enforce proper behavior and avoid mistakes. If a breach does occur, monitoring privileged account use also helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cyber security threats.

Detect

Ensuring visibility into the access and activity of your privileged accounts in real time will help spot suspected account compromise and potential user abuse. Behavioral analytics focuses on key data points to establish individual user baselines, including user activity, password access, similar user behavior, and time of access to identify and alert you of unusual or abnormal activity.

Respond

When a privileged account is breached, simply changing the password or disabling the account isn't sufficient. While inside, hackers could have installed malware and even created their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that your entire Active Directory is impacted and investigate and make changes so the attacker can't easily return.

Review and Audit

Continuously observing how privileged accounts are being used through audits and reports will help identify unusual behaviors that may indicate a breach or misuse. Automated reports help track the cause of security incidents as well as demonstrate compliance with policies and regulations. Auditing of privileged accounts will also give you metrics that provide executives with vital information to make more informed business decisions.

In conclusion, implementing an identity security program and implementing best practices is crucial for protecting sensitive data and preventing data breaches. By taking proactive measures to secure their systems, organizations can ensure the safety of their customers' information and comply with data privacy regulations.