STUDENT

The Institute of Internal Auditors

Data Risk in Third-party Ecosystem

Arnab Banerjee

Student, GRMI
Batch No. 11
Email:
arnabbanerjee@grmiclass.com

Businesses depend more on third-party ecosystems for efficient operation in today's interconnected world. These external organisations that provide products and services to the organisation are referred to as ecosystems, together with suppliers, vendors, contractors and other parties. Even though third-party ecosystems can be very beneficial to businesses, many risks are also involved, especially when it comes to data.

In order to secure data from unauthorised access, use, or disclosure, which is one of any organisation's most precious assets, it is imperative to implement appropriate security measures. However, when an organisation shares data with third-party organisations, it may be more exposed to various data risks, such as breaches, exploitation, and data loss.

Data Breaches: These are among the most serious threats connected to third-party ecosystems. It is possible that third-party organisations do not take data protection as seriously as the organisation does, or they may have liberal security procedures. Their vulnerability to phishing, hacking, and other cyberattacks may result from this. Sensitive data may be disclosed in the event of a third-party business breach, which could harm the organisation's reputation and have serious financial and legal repercussions.

Misuse of Data: This is another danger posed by third-party ecosystems. Third parties can access the information they do not require or use it in ways the organisation has not approved. An example would be a vendor using client information for marketing without getting consent from the company.

Data Loss: Accidental deletion, technology failure and natural disasters are just a few ways data loss can happen. Since these third-party organisations might not have the same level of backup and recovery capabilities as the organisation itself, the risk of data loss increases when data is stored in third-party ecosystems.

Data governance policies that define who has access to sensitive data and how it can be used should be put in place by organisations to reduce the risk of data misuse. To ensure that third-party organisations are aware of their responsibilities and obligations concerning data protection and privacy, they should also offer training and awareness programmes. Contractual agreements that specify the conditions of data use, confidentiality, and security should also be in place within organisations.

Organisations must ensure that third-party entities have sufficient backup and recovery procedures in place in order to reduce the risk of data loss. In addition to regular data backups, this also entails backup strategies for potential data loss scenarios. Organisations should constantly review third-party backup and recovery strategies to make sure they are current and efficient.

When it comes to third-party ecosystems, data privacy and compliance are crucial factors to take into account. Organisations need to confirm that third-party companies are adhering to all applicable data protection and privacy laws, such as GDPR, CCPA, and HIPAA.

Organisations should routinely audit and evaluate outside parties to make sure they are abiding by legal standards in order to reduce the risk of non-compliance. Additionally, they must ensure that any contracts they enter into with third parties contain clauses requiring them to adhere to applicable laws governing data protection and privacy.

Final thoughts In third-party ecosystems, data risk is a major concern, and in order to safeguard their priceless data assets, organisations must adopt a proactive approach to data risk management. This entails carrying out extensive due diligence on third-party companies, putting data governance policies into place, offering training and awareness programmes, and ensuring compliance with pertinent laws. Organisations can assist in safeguarding sensitive data by employing a comprehensive strategy to data risk.