Ouch-proof Data Migration Plan: Ensuring Security and Data Integrity

Migrating to Microsoft 365, consolidating data centers, and upgrading systems all have the potential to drive efficiency and strengthen collaboration. But the migration process may also involve risks to essential business data. Take control of this critical element of your data migration plan: ensuring security and data integrity.

Migrations do increase the risk that data will become corrupted, lost, or vulnerable to unauthorized access. However, with careful planning and the right tools, organizations can proceed with confidence. Following best practices before, during, and after migration mitigates risks and helps to ensure a successful migration.

Know the Risks

Moving data from one location to another increases the risk of data breach for several reasons. In the first place, multiple touchpoints along the way mean additional opportunities for cyber criminals to exploit potentially weakened security protocols. And data in transit requires additional security to guard against interception attacks.

Secondly, employees and third parties that normally do not have data access may temporarily need a certain degree of access to accomplish the migration. This increases the possibility of insider threats. It

also raises potential compliance issues, depending on the data protection laws governing the organization and its data.

Migration also increases the risk of data corruption and data loss. For instance, data can become corrupted due to compatibility issues or transfer errors. Likewise, an incomplete data transfer or data duplication may lead to inaccurate analytics and reporting in the new system. And unexpected technical glitches or human errors during transfer may result in lost data.

Before: Essential Preparation

Safely navigating these risks begins in the preparation process. The migration team should:

- Conduct a thorough data assessment – Take an inventory of your data. Know what data you have, identify sensitive data, and know where it will live in the target system. This empowers the team to prioritize and implement appropriate security measures.
- Clean up your act – Avoid migrating a mess. Ensure that source systems are validated and checked for errors. Deduplicate and correct errors as much as possible with your source data. This will reduce the risk of post-migration issues and improve overall data quality.
- Carefully choose migration tools – Select migration tools that offer robust security features and that are compatible with both the source and destination systems. The tools should provide logs and reports for auditing processes, including a non-migrated data report.
- Ask the right questions – Choose a migration partner with a proven track record around security. Ask about the process and whether data will be buffered at any point. Also discuss data

integrity expectations. While no solution can guarantee complete data integrity, setting expectations and planning for possibilities improves the results.

- Assess the risks – Make sure to account for special considerations such as compliance requirements, unusual workflows, highly sensitive data, and so forth. Additionally, understand the limitations of the target system. For instance, Exchange Online has a maximum mailbox size of 150GB.
- Back up your data – Be sure to back up all data prior to migrating and test the backup to confirm the data can be restored accurately and completely.

During: Security Through the Journey

Data becomes particularly vulnerable in the process of moving from one location to another, and bad actors know that. This becomes particularly important if data is being buffered in a third-party location, rather than going directly from the source location to the target. Therefore, ensure strong encryption of all communications between the source and the target.

Additionally, during migration limit data access according to the principle of least privilege. Employ strong authentication methods and network security and monitor logs to prevent unauthorized access.

Keep compliance obligations top of mind during migration and ensure that the process complies with all relevant laws and regulations. Also, maintain comprehensive documentation of the migration process. This should include any issues and an explanation of how they were resolved.

After: Verification Is Key

Once the migration process has completed but before going live, thoroughly validate data integrity. Data validation tools will allow you to ensure the accuracy and completeness of your transferred information. Identify and address any discrepancies.

Then continue to monitor the data and systems for any irregularities or security breaches. Continuous monitoring will help the migration team to quickly highlight and minimize any post-migration issues.

Data Migration Plan: Ensuring Security and Data Integrity Easier with the Right Partner

Partnering with data migration experts like those at Messaging Architects helps to ensure a smooth and secure migration process. Our consultants bring proven tools and experience honed through hundreds of successful data migrations. And we migrate behind the scenes, ensuring a positive experience for both end users and IT staff.