Unit 10: DR Solutions Design and Review

Tobi Zeier, September 2024
University of Essex Online

Part A

Read Opara-Martins et al (2014) and Morrow et al (2021) and answer the following questions:

1. What are some of the main vendor lock-in issues the authors identify? How would you mitigate them?

   Issues
   - Lack of Interoperability: Providers use proprietary standards and APIs, making it difficult for systems to work across different platforms.
   - Portability Issues: Proprietary data formats hinder organisations from easily moving data or applications between cloud providers.
   - High Switching Costs: Migrating between providers is expensive and time-consuming.
   - Lack of Standardisation: The absence of industry-wide standards increases dependency on individual providers.
   - Legal Lock-in: Contracts often restrict customers, making it harder to switch providers.

   Mitigations
   - Promote Interoperability: Use standard APIs (e.g. open source) to ease integration across platforms.
   - Enhance Portability: Use standardised data formats to simplify migration.
   - Plan Exit Strategies: Review contracts carefully and plan for provider changes.
   - Support Standardisation: Encourage industry-wide standards to reduce lock-in

2. What are some of the security concerns with the modern cloud? How can these be mitigated?

   Concerns
   1. Unsecured Cloud Storage: Misconfigurations, such as in AWS S3 buckets, can expose sensitive data to unauthorised access, leading to breaches.
   2. Weak Access Control: Poorly managed access rights can allow hackers to gain unauthorised entry, as seen in the OneLogin breach where AWS keys were compromised.
   3. Ransomware Targeting Cloud Backups: Attackers increasingly target cloud backups, using ransomware to steal or destroy data.

4. Supply Chain Attacks: The SolarWinds attack exploited on-premises systems to infiltrate Microsoft 365 cloud environments.

Mitigations

- Due Diligence: Ensure cloud services are properly configured, with secure access policies and encryption.
- Manage Access: Use multi-factor authentication and limit access based on roles.
- Data Protection: Encrypt data both at rest and in transit, with regular security audits.
- Monitor and Defend: Continuously monitor cloud systems and collaborate with providers to detect unauthorised activities.

References:

Opara-Martins, J., Sahandi, R., & Tian, F. (2014) 'Critical review of vendor lock-in and its impact on adoption of cloud computing', *International Conference on Information Society (I-Society 2014)*. London, UK, 10-12 November. IEEE. 92-97.

Morrow, T., LaPiana, V., Faatz, D., & Hueca, A. (2020) Cloud Security Best Practices Derived from Mission Thread Analysis (Version 1). Carnegie Mellon University. DOI: https://doi.org/10.1184/R1/12363563.v1