DR Solutions Design and Review

Introduction

Kumar identifies cloud vendor lock-in as a structural risk created by proprietary cloud ecosystems, limited interoperability, and contractual constraints. The author highlights many aspects of vendor lock-in which are not exclusively a technical concern, but one that also arises from governance, architectural decisions, and organizational dependency on provider-specific services. Effective mitigation therefore requires early planning, architectural discipline, and strategic risk management.

(Kumar, 2024)

Corbari et al., presents frameworks such as Mission Engineering Thread (MET), Mission Thread Analysis (MTA) and more additional frameworks, which are further developed concepts adapted from the DoD (Department of Defense) and are designed for aligning operational objectives, systems, and cyber risk, while not directly address vendor lock-in in the public service, the document is more focused on cyber framework from a military standpoint, the framework focus mainly on three elements; Persona, Logical and Physical and provides a structured method for understanding dependencies and prioritizing cybersecurity decisions based on mission impact, together, these works emphasize the importance of visibility, traceability, and intentional design when managing complex digital ecosystems.

(Corbari et al., 2024)

Vendor Lock-In Issues Identified by Kumar

The author organizes vendor lock-in into multiple interconnected dimensions that may influence organization complexity and lead to an increased operational risk.

Technical Lock-In

Cloud platforms encourage deep integration with proprietary services, APIs, and data formats. Applications development based on these services become challenging to migrate without substantial refactoring and a limited compatibility between providers further contributes to the cost and complexity of changing environments.

Organizational Lock-In

Standards and security models that are vendor specific, reduce portability and interoperability. When operational processes, security controls, and skillsets are designed to a single provider, organizations become dependent on the vendor’s architecture, making transition much more complex, riskier and more disruptive.

(Kumar, 2024)

Legal and Contractual Lock-In

Kumar also emphasizes the contract related limitations, binding service agreements and compliance obligations that are linked to specific providers or regions, these factors can create financial penalties, regulatory challenges, and operational barriers that discourage or delay migration.

(Kumar, 2024)

Business Risks

The overall impact of such lock-in means includes in between; higher costs, reduced innovation, limited bargaining power, increased operational risk and challenges related to data portability and governance.

(Kumar, 2024)

Mitigation Strategies for Vendor Lock-In

The author proposes several strategies to reduce exposure to vendors lock-in, for instance; proactive exit planning where organizations should define exit and migration strategies early, identifying dependencies and constraints before they become critical.

(Kumar, 2024).

Multi-Cloud Strategies

Reduction of reliance by distributing workloads across multiple providers and not on a single vendor, though it requires careful governance. Containerization could help keep application portability using packaging, what enables workloads to run across different cloud environments with minimal change.

(Kumar, 2024)

Infrastructure as Code (IaC)

Declarative infrastructure definitions support repeatability and portability across platforms, data portability and decoupling helps avoid proprietary data formats and designing loosely coupled systems based on open standards reduces dependency on vendor-specific services.

(Kumar, 2024)

Mission Thread Analysis and Security

The article by Corbari et al. does not explicitly address vendor lock-in; however, vendor lock-in represents an implicit and significant risk within the context examined. Although vendor lock-in is not the central focus of the study, Mission Thread Analysis (MTA) exists precisely to identify and mitigate mission risks arising from vendor-dependent, opaque, and proprietary dependencies. In this sense, the article contributes a complementary perspective by providing a framework capable of revealing such latent dependencies. The author emphasizes that cybersecurity decisions must be grounded in mission priorities and shared understanding among stakeholders, concepts such as Mission Engineering Thread (MET) and Mission Thread Analysis (MTA) are among other concepts that enable organizations to trace how system dependencies, including cloud services, support mission outcomes and where failures would have the greatest impact, by focusing on multiple mission-critical functions such as Persona (Users, Policies, Programs), Logical (Services, Routs, Switches) and Physical (Systems, Locations, Infrastructure), rather than isolated technical components, the approach helps support informed decision-making about threat, risk, resilience, and resource allocation.

(Corbari et al., 2024)

Conclusion

Kumar shows that cloud vendor lock-in presents are a multifaceted risk rooted in technical design, organizational practices, and contractual obligations and the mitigation relies on proper and early architectural foresight, portability, and governance rather than reactive migration efforts.

(Kumar, 2024)

Corbari et al., contributed to this view by providing a mission focused framework that supports institutions understand and manage many of the complex dependencies' aspects, altogether, these works underscore the need for calculated design and mission-aware risk management in modern cloud-dependent environments.

(Corbari et al., 2024)

References

- Kumar, Aashish. "Cloud Vendor Lock-In: Identify, Strategies and Mitigate" (2024).
- Corbari, G.I., Khatod, N., Popiak, J.F. and Sinclair, P., 2024. Mission Thread Analysis: Establishing a Common Framework. The Cyber Defense Review, 9(1), pp.37-54.