Unit 10: Practical Applications and Issues in DR Implementations (Seminar 5: DR Solutions Design and Review).

E-Portfolio Activity

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?

Response:

According to Opara-Martins et al (2014), Vendor lock-in by cloud computing service provider refers to a situation where clients are stuck with a cloud service provider and the cost of switching to another provider is high. It is characterized by expensive and time-consuming migration of application and data to alternative providers that might include business disruption experience. The vendors implement this mechanism through Contract/Service Level Agreement (SLA), a joint survey by Cloud Security Alliance (CSA) and Information System Audit and Control Association (ISACA) identified exit strategies, contract lock-in and Data ownership as major concern by companies .

The main vendor lock-in issues identified by the author in the articles are as follows:

- Lack of interoperability: According to National Institute for Standards and Technology (NIST), Interoperability is the ability of cloud computing services from different providers and other applications or platforms are not cloud dependent and can seamlessly exchange assets. However, vendor lock-in promotes lack of interoperability and the providers achieves it by building a closed system or application architectures that is not compatible with other cloud service providers and they don't comply with the standard API that allow higher cloud layer link, exchange, and interact to a range of other service providers thereby making alternative vendor switch cost very expensive and complexity of application integration.

- Lack of portability: The author defined portability as the ease of ability to which application components are moved and reused elsewhere regardless of the provider's platform, operating system, infrastructure, location, storage, data format or APIs etc example of the cloud computing migrations are Platform-as-as-Services (PaaS), Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS). The vendor uses licensing the software application under exclusive condition to lock-in clients and this increase the provider's bargaining power and other parameters over the clients. Also, each providers develop its own specific technology solution, remote APIs or new programming languages thereby making it difficult for client to port to alternative providers. Example is an enterprise utilized Amazon Quicksight for data visualization, it will be difficult to relocate its data to a service competitor with extensive redevelopment and testing because the services are exclusive to AWS which promotes over dependence on a single vendor.

- Lack of Standardization: This is a disadvantage when a client wants to migrate, integrate or exchange of cloud computing resources. it opposes agility, efficiency and the low cost associated with utilization of cloud-base services. Example when there is no standard that address workload migration and data migration format. It will make it difficult for data portability and interoperability.

- Technical Barries: Vendor lock-in comes with various technical barriers such as integrations challenges of data and applications across clouds where cost and complexity of developing and maintaining integration between platforms with disparate interfaces and protocol can easily erase the economic and efficiency gains of cloud computation. Vendors configures and customize solution that the cost-benefit to port to alternative vendors will not worth it

In addition to the above, according to article publication of Geeks January 2023, other challenges of vendor lock-in include limited flexibility where single cloud provider hampers benefit from new technologies or lower prices offered other providers, dependence on single providers might lead to great chances of service interruption or outages if supplies run into technical issues, it limits scalabilities that ability to expand and develop its capabilities.

Mitigation of Vendor Lock-in

- Multi-cloud or hybrid strategy: This is achieved by utilizing various cloud service providers for various applications which gives an organisation the flexibility of choosing service providers and lowering chances of being overly dependence on one source and hybrid solutions offers agility (Carrol,J 2023).

- Utilizing standard-based solutions: Standardization supports applications among cloud service providers to interoperate with one another, exchange and cooperatively interact with data as well as protocol for joint coordination and control. It is critical to evaluate vendor compliance with standardization before utilization of its application.

- Data portability: it is important to consider vendors that its applications model allows data and content migration among other providers without disruption of data availability or other services. This will guarantee that data is not linked to a particular provider, and it will be easy to switch providers.

- Service Level Agreement (SLA): The organisations should discuss the SLA with the provider to ensure specific level of service availability and it allows smooth exit in the event of dissatisfaction with provider.

- Open-Source Technologies: The organisations can employ open-source technology which is free to use and modify and are not dependent on a single provider. It increases the degree of control an organisation has over its technological stack and reduces the challenge of relying on one source.

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

Response: There are risk, threats, and vulnerabilities that faces Cloud-based application and system security, below are examples of such threat experienced by Cloud Service Providers (CSP).

- Unsecured storage service (AWS): This is cases of unauthorized exposure of data to the internet have been linked to improperly application configuration. The access policy on AWS S3 bucket was improperly configured, allowing public access to data in the bucket. The press reports on this incident suggested that misconfiguration of AWS resources by consumers is a common challenge.

- Email compromise (Deloitte): This is where attacker access a firm e-mail system through use of a compromised system administrator credential. This happened to Deloitte on its email system hosted on Microsoft Azure, where the administrator’s account uses only a password for authentication of access.

- Ransomware leverage the cloud: This is where cloud-base back-up software was targeted and used by Doppel-ware and Maze ransomware operator to steal or destroy backups as a normal tactic during attacks [Abram 2020].

In addition to the above, EC-Council Cybersecurity Exchange stated that as a cybersecurity professional, it’s important to be aware of the security threats, issues, and challenges your customer’s or employer’s cloud infrastructure faces and some of the most common ones include:

- Security system misconfiguration
- Denial-of-Service (DoS) attacks
- Data loss due to cyberattacks.
- Unsecure access control points
- Inadequate threat notifications and alerts

Mitigations or best practices to Modern Cloud Risk, Threats, and Vulnerabilities

- Perform Due Diligence: This requires an organisation that wants to use cloud-base services to examine and fully understand the security implications of deploying or moving applications and systems to a CSP.

- Managing Access: it involves identification of different categories of users in a cloud-based IT environment, determining the responsibilities of each user category and ensuring access to resources are controlled to protect the resources from unauthorized user.
- Data Protection: This prevents the accidental or authorized disclosure of data and ensures continued access to critical data in the event of errors, failure and compromise.
- Monitor and Defend: it requires the CSP and cloud-based consumers to work together to monitor cloud-based systems and applications to detect unauthorized access to data or other cloud resources.

Reference:

EC-Council Cybersecurity Exchange (2022)What Are the Top 5 Cloud Computing Security Challenges?. Available from :https://www.eccouncil.org/cybersecurity-exchange/cloud-security/what-are-the-security-challenges-in-cloud-computing/#:~:text=Common%20Cloud%20Computing%20Security%20Risks&text=Security%20system%20misconfiguration,Unsecure%20access%20control%20points [Accessed 08 October 2023].

Geeks (Jan 27 2023). Vendor Lock-in in Cloud Computing. Available from:https://www.geeksforgeeks.org/vendor-lock-in-in-cloud-computing/ [Accessed 05 October 2023].

Morrow. el at (2021), Carnegie Mellon University Software Engineering Institute, Cloud Security Best Practices Derived from Mission Thread Analysis.Available from: https://apps.dtic.mil/sti/pdfs/AD1139951.pdf[Accessed 08 October 2023].

Opera-Martins et al (2014). International Conference on Information Society (i-Society 2014) Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing.Available from:https://eprints.bournemouth.ac.uk/22467/1/Critical%20Review%20of%20Vendor%20Lock-in%20and%20Its%20Impact%20on%20Adoption%20of%20Cloud%20Computing.pdf [Accessed 04 October 2023]