**Unit 4 Seminar:**

**Activity 1: DR Terms and Concepts**

1. **What is the difference between Hot Standby, Warm Standby and Cold Standby? Frame your answers in terms of availability, RPO and RTO.**

Hot standby takes over processing immediately when the primary site is down, meaning that time to restore service (RTO) is very short, usually within seconds. Conversely, cold standby requires more intervention to install necessary dependencies, such as applications, operating systems, and hardware, which means that possible data loss is increased (associated with RPO). Warm standby lies between hot and cold standby, with the backup system remaining partially active at a lower cost compared to hot standby (Alhazmi & Malaiya, 2013).

1. **Does the technology deployed affect the options available? For example, can you create a high availability, hot standby solution between two on-premise data centres?**

The technology deployed doesn't affect the options available, as for example synchronous replication of data centers provides high availability and ensures no-data-loss disaster recovery. Additionally, cloud technologies provide a pay as you go pricing model, ultimately enhancing the best possible ration between cost and availability. (Pachot, 2023)

**Activity 2: DR Solutions Design**

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

The authors point out increased expenses and time-consuming migration, caused by designing systems that are incompatible with software developed by other vendors and designing a closed architecture that lacks interoperability with other applications. Another issue originates from licensing the software under exclusive conditions.

To avoid the above issues, the authors highlight the importance of pressuring cloud providers to support interoperability (Opara-Martins et al, 2014). At the present, the number of cloud services has increased immensely compared to ten years back; therefore, the problem of interoperability has been profoundly reduced. The authors also point out the importance of standardization, which has reduced interoperability issues. At present, cloud advancements over the last few years have led to immense competition in the market, ultimately increasing the need for flexible solutions tailored to businesses, consequently reducing the vendor lock-in issues.

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

One of the security concerns is improperly configured services, leaving data exposed to adversaries. This was the case happened to AWS Storage Services, where records of customers were exposed to the public internet. Another security issue exposed by AWS happened when an error in maintenance procedure caused drop in network bandwidth, consequently losing block of storages. Another cloud security issue happened to Deloitte, where the adversaries gained access to the firm’s email system, through compromised system administrator credentials (Morrow et al, 2021).

According to the authors analysis, there are four important practices to avoid risk of incidents:

1. **Performing due Diligence**: Meaning that cloud consumers should fully understand the security implications of deploying or moving applications and systems to a Cloud Service Provider.
2. **Managing Access:** Resources should be protected from inappropriate or unauthorized use. This can be ensured through determining the responsibilities of each user category, and ensuring access to resources is controlled.
3. **Protecting Data:** Preventing the accidental or unauthorized disclosure of data
4. **Monitoring and Defending:** To detect unusual events.

**References:**

Alhazmi, H., O. & Malaiya, Y., K. (2013) Evaluating Disaster Recovery Plans Using the Cloud. Colorado State University. Available from: <https://www.researchgate.net/publication/244478078_Evaluating_Disaster_Recovery_Plans_Using_the_Cloud> [Accessed 6 July 2024]

Morrow, T., LaPiana, V., Faatz, D., Hueca, A. & Richmond, N. (2021) Cloud Security Best Practices Derived from Mission Thread Analysis. Software Engineering Institute. Available from: <https://insights.sei.cmu.edu/documents/1283/2021_005_001_551472.pdf> [Accessed 7 July 2024

Pachot, F. (2023) Achieving High Availability and Disater Recovery with Two Data Centers. YugabyteDB. Available from: <https://www.yugabyte.com/blog/high-availability-disaster-recovery-two-data-centers/> [Accessed 6 July 2024]