7 Mistakes That Newcomers To Cloud Make

With IT modernization gaining pace, a large number of organizations are turning towards adopting cloud.

It is only natural how cloud has emerged to be the most viable option for any corporation that puts flexibility, enhanced security, storage, and scalability upfront. **Recent survey reports** indicate more than 90 percent of enterprises are switching to a multi-cloud strategy. Another 87 percent have a hybrid cloud strategy option in place.

Furthermore, 59 percent of enterprises are expected to switch to the cloud in the wake of COVID-19 turning into an epidemic. The Ministry of Transport and Communications, Qatar, has signed an agreement with Microsoft to set up an **Azure datacenter** in Qatar. In essence, it all boils down to cost-effectiveness and agility where cloud promises a productive edge for organisations at large.

However, in most cases, newcomers to the cloud are prone to making a handful of mistakes that lead to failure and significant loss of money and time in tandem.

Owing to the cross border nature of cloud services coupled with its unique architecture, Qatar's **Personal Data Privacy Law(13)of 2016** along with **National Information Assurance Policies** demand all communications and transactions to be dealt with from a different perspective. This is even more evident in case of newcomers to cloud.

In this post, we take a close look at 7 common mistakes that newcomers to cloud are known to make, and how you can go about avoiding it.

1 Unnecessary Switchover from One Vendor To Another

One of the most common mistakes that corporations make is switching vendors unnecessarily. It is to be understood that not all cloud providers are the same. In case, your organisation is looking to make a move towards public cloud from private, it is advised by all means that you stick to your current vendor. According to **RightScale**, the average business runs 38% of workloads in public and 41% in private cloud. Switching from one Vendor to another will not only cost you extra time to manage relationships, but the coordination will be difficult, as well.

If your primary need is data storage, you might as well explore the options provided by your current vendor. This not only saves time but also lessens the hassle that is usually associated with numerous organisations, switching vendors only due to a lack of ignorance towards the options that their current provider is capable of.

Whether you are facing a security or compliance issue, it's in the best of the interest to talk it out with your provider and explore other options that deem fit.

2 Migrating it Altogether

Given the latest technological advancements, the cloud migration has become seamless. However, that doesn't rule out the possibility of a mishap in the event of a lack of knowledge or training for higher-level management.

When looking to migrate to cloud, go by the word of the experts. It is strongly recommended that you migrate in parts and not as a whole entity. Start with a few applications during the early phase and pace up accordingly.

In case there occurs a glitch in the migration, you will be on the safe side with your larger data. Additionally, migrating in parts also puts in a better place with troubleshooting apps that are of utmost necessity.

If you run a financial or healthcare firm, you are running a large amount of data that is subjected to interoperability across a critical cluster of applications. Hence migrating to a new environment can throw in stiff challenges on the lines of security or compliance. Thus, moving in parts is a safe and secure way to do it.

3 Not Viewing Security as a Shared Responsibility

For newcomers to the cloud, they tend to assume that the CSP is liable to handle all security aspects. Little do they understand that despite their migration to cloud, the organization is still accountable for their own security.

Simply put, cloud security is invariably a shared responsibility, and everyone should be doing their bid to keep things safe. The only way to go about it is to develop capabilities that can help manage risks at hand, and capability is best formed of people, and processes, and at a later stage by the tools prepared by them. Qatar 2022 Cybersecurity framework also highlight the need of understanding the shared responsibility as a prerequisite before migrating to Cloud.

Besides, the policies for cloud governance and security enhancements impart your organization with the necessary guarding that can help you operate efficiently. As such the tools you use for security matters the most as they help you get detailed analytics to help prevent violations, risks and other complications, drive enforcement, and finally offer quarantine in the face of a breach.

4 Overlooking The Security Aspect For Entire Supply Chain

External supply sources can bring about a wide number of threats.

For instance, a large number of organizations in Qatar make use of a number of codes hosted public libraries. Although such an approach helps develop applications a lot faster, using codes of unknown provenance, without adequate understanding and verification can make way for insecure applications.

From a broader perspective, the issue isn't restricted to organizations migrating to Cloud newly, but for major enterprises across Qatar. This is primarily, because it's not always feasible to verify the security of the codes in use. However, adopting such a practice keeps security issues at bay.

Thus, we have to always ensure that the tools that you utilize from an outside source (code, hardware, software) is effective and reliable.

5 Ignoring Security Paradigm Shift

Unlike on-premises security considerations, Cloud Security be a

paradigm shift as you will have to secure the data and identity, making identity the new perimeter. Failing to understand necessary security considerations can slow down cloud migrations while impacting digital transformation initiatives.

Qatar 2022 cybersecurity framework and MoTC's Cloud Security Policy is good starting point for organizations to make sure that they possess necessary capabilities and readiness before migrating to cloud.

6 Restricting Access For Cloud Platforms

One of the most essential concerns of Cloud security is access control. Now, only authorized personnel should have access to Cloud platforms and the level of rights required to carry out the functions of their role.

To maintain security, an enterprise attempting to embrace Cloud new should thereby go forward with a privileged access protocol. In essence, such an approach will help identify all forms of access required for the system to ensure applications of control meeting first had system requirements ranging across public websites that are open for access, other authenticated access for any internally used applications, and highly controlled access accounts that require special privilege to all applications and data.

Lastly, there should be processes in place to help lessen the exposure ensuring only users with proper admin rights have access to required Cloud data and allied applications. This shall enable wholesome management of an entire account cycle right from the time it's created to when it's no longer needed and can be deleted.

7 Over Usage of Admin Accounts

When signing up with a cloud provider, the root account is generally the first account that one creates. It's the most privileged account ever, containing access to all aspects of an organization's cloud network.

As such, when the admin account is compromised, it puts the entire cloud network in jeopardy. This is exactly why one needs to limit the admin access for users and strictly keep it reserved only for the utmost necessary tasks.

Never allow users to use the root account for daily tasks as it puts you at more risk of being exposed to malware, thus leading to a dent in the security system.

Key Takeaway

Now that you know the common mistakes that people make while migrating to the cloud, you should be in a better position to retrace your steps. The idea is to steer clear of any propaganda revolving around the industry.

Don't just follow the herd blindly. Rather, access your needs, get your findings right, reconsider your requirements, and discuss the inherent risks and challenges that you might have to deal with.

Only then you will be in the right position to make a call. While cloud computing is the next big thing, you should always make efforts to mitigate errors and minimise costs at all levels. That being said, you can make the best out of your cloud migration process.