WHY STABILITY IS KEY FOR CLOUD

DIGITAL BUSINESSES CANNOT AFFORD TO HAVE UNAUTHORISED DATA ACCESS IN THE CLOUD NOR HAVE THEIR CLOUD SERVICES PROVIDER UNEXPECTEDLY SHUT DOWN SHOP, SAYS YASSER ZEINELDIN, CEO, EHOSTING DATAFORT.

At the start of this decade, many regional IT managers expressed concern whether their organisations would ever embrace cloud as a platform or not. They mused that cloud is perhaps suitable for very specific workloads, but they would never migrate these mission critical workloads to an external platform. As we move into the next decade, much of the regional mindset has changed to embrace cloud as a business enabling platform, while keeping mission critical workloads on a private cloud or even hybrid cloud platform.

The sheer cost and agility advantages of the public cloud platform is driving regional IT spending into this area at a double-digit growth rate. The requirements of in-country data regulations and compliance is attracting large cloud providers to invest locally. And such players are increasingly investing inside the region and in countries like the UAE and Saudi Arabia, in a relatively steady but consistent manner. According to global research and consulting firm Gartner, the number of Managed Cloud Services Providers is predicted to triple by 2020.

So, all seems to be well established for rapid movement forward into the realm of wide spread cloud adoption and migration. But global risk and cybersecurity executives continue to

> THE SECOND AREA OF RISK IS AROUND THE ECONOMIC, FINANCIAL AND TECHNOLOGY STABILITY OF THE CLOUD HOSTING PROVIDER AND ITS ECOSYSTEM OF SUPPLIERS.”

IT AND CYBERSECURITY MANAGERS MUST ENSURE THAT THE SAME LEVEL OF COMPLIANCE AROUND SECURITY POLICIES AND EMPLOYEE SIGN-ON THAT EXIST ON-PREMISES ARE MAINTAINED FOR CLOUD PLATFORMS AS WELL."

remain concerned about relatively weak security controls and policies that exist across emerging cloud-data platforms in general. According to Gartner's latest Emerging Risks Report and Monitor, the majority of risk executives reported being most concerned about were the probability and impact of potential data risks associated with cloud computing.

While adoption and migration of cloud delivers immediate CAPEX and OPEX benefits and brings agility into the organisation, IT and cybersecurity managers must balance the speed of adoption with increasing levels of control and compliance into the cloud. Institutional and country level audits like GDPR, punitive measures by the Board, and other corporate shareholder guidelines, do not allow any lack of rigour by IT and cybersecurity managers in this area.

For enterprises that are actively moving to the cloud, there are the two principal risk areas that need to be actively monitored going forward. The first area of risk is the migration of on-premises data to cloud platforms and this could include sensitive, private and confidential information as well as historical transactional data about the organisation, its suppliers as well as its customers.

IT and cybersecurity managers must ensure that the same level of compliance around security policies and employee sign-on that exist on-premises are maintained for cloud platforms as well. They must know where the data is resident and who is responsible for the migration and movement of the data to cloud platforms. Once resident on the cloud, they must remain in control and responsible for who has access to data in the cloud. The cloud data access policies must remain mirrored to the on-premise policies and it is the IT and cybersecurity managers who are responsible for this in-cloud compliance.

The second area of risk is around the economic, financial and technology stability of the cloud hosting provider and its ecosystem of suppliers. Rapid migration of data to the cloud is driving the spawn of gold-rush Cloud Service Providers, either as direct or indirect players. IT and cybersecurity managers must be particularly concerned if their Cloud Services Providers change their Service Level Agreements or display any evidence of inability to provide their services.

The combination of the above two risks, namely unauthorised access to cloud data and inability to provide cloud services, due to lack of compliance by either the organisation or the Cloud Service Provider, can have disastrous consequences for the organisation. While such an extreme situation is yet to occur in the region, global advisory firms like Gartner are drawing attention to the possibility, as an emerging data risk in cloud computing.

As a corollary, end-users are advised to engage with economically stable and well-entrenched Cloud Services Providers, while the gold-rush is ongoing.