INDUSTRY Q&A: HOW THE CLOUD CAN ENHANCE BUSINESS RESILIENCY

Cybersecurity expert John Muoio discusses cloud migration in times of crisis

June 12 2020 • Security Info Watch • Steve Lasky

For remote workers, having greater control over their work environment is a huge advantage of working virtually. However, that control can bring more responsibility, and oftentimes, greater cybersecurity threats to organizations. It's now up to employers to make sure data is stable, secure and readily accessible. To meet this demand, several businesses have widely embraced the cloud to support their growing infrastructures - further demonstrating that moving business operations to the cloud should be the first step in your business resiliency plan. John Muoio, Technology Solutions Manager at VAI, expands on how businesses can seamlessly move to the cloud and give their teams safe, secure and reliable access to the systems and data they need, wherever they're located.

Why should moving business operations to the cloud be the first step in an organization's business resiliency plan?

As businesses begin to adjust to a new normal over the next few months, companies and employees are wondering what the new normal may look like. The reality is, business certainly will not be the same as it previously was and organizations must reinvent themselves in order to survive.

In the past, companies traditionally relied upon an on-premise business model that required face-to-face interactions. This method of collaborating with employees can sometimes be a hindrance. In order to update a strong business resiliency plan, companies must invest in a secure, solid foundation that enables them to seamlessly communicate and work remotely – which can be enhanced with cloud technology. Today, many businesses have set up their workforce to work remotely, having had the need to do this quickly, and the cloud has become an essential technology for many of these companies. Having a cloud infrastructure will allow employees to easily work remotely and frees up internal technical resources required to implement, monitor, and support this environment. Alternately, by utilizing the cloud as the first step in your business resiliency plan, your company will have the fault-tolerant infrastructure needed for leveraging other critical applications such as e-business, customer portals, mobile applications, and remote collaboration tools.

What benefits will businesses see by transitioning to the cloud?

The ability to host applications in the cloud and access your data from almost anywhere in the world is vital for your business continuity as remote work continues. By transitioning to the cloud, businesses can streamline their departmental functions and deliver optimized performance and significant cost savings. The cloud also provides scalability and flexibility. By investing in a cloud solution, businesses can add additional storage, memory, or processing power with zero disruption - eliminating the need to purchase new servers or upgrade operating systems to enable additional features or functions. Therefore, there will be no need for businesses to spend money on hardware, software, or licensing fees.

With workforces operating remotely, the cloud can also enable faster deployments. Businesses must have cloud infrastructure and equipment in place so no lead time for equipment acquisition is required. This enables projects to start faster and end sooner. In addition, since consumers and businesses have adopted tools such as smartphones and tablets, the ability to host applications in the cloud and access it from anywhere and at all times, is quickly becoming vital.

What challenges will companies face when migrating to the cloud and how can they navigate these issues?

The main challenge for businesses will be to properly plan a cloud migration strategy. IT departments should not deploy cloud technology with their infrastructure without a solid strategy in place. This includes evaluating and selecting the right cloud provider. Businesses need to also consider costs, minimize or eliminate downtime, evaluate employee training, and estimate time to complete the migration. While a business might be eager to migrate their data to the cloud, they need to know which data should be prioritized and secured. A typical best practice is to deploy a prototype or proof of concept application first. This way, your employee can test the security and functionality of the cloud deployment before the larger-scale deployment.

Cloud security is imperative. Security is the number one planning step in adopting the cloud, so it must be a top priority - especially when integrating new technologies or deploying to a public cloud. Businesses must invest in a cloud solution that adds the latest in security beyond most businesses' capabilities and automatic updates without the need for downtime. Businesses that move to a cloud solution can add the latest securities beyond most business capabilities and also enable automatic updates without the need for downtime.

What tools should organizations invest in to help seamlessly move business to the cloud?

Organizations must evaluate cloud providers who offer cloud migration tools. Cloud migration tools can automate reproducible periodic data migrations, whether moving to public, hybrid, or private environments. The cloud migration tool directly impacts the timeline of the business transformation.

When selecting a third-party cloud migration tool, companies should look at the size and amount of content they are hoping to transfer, their ideal migration timeline, and budget and cost range, as well as customer needs if a migration needs any customization, like specific security compliance measures. After considering these four aspects, companies can select a cloud migration tool that best fits their needs or combine tools to create the most efficient solution. Therefore, it's important to choose tools that are reliable and customizable.

As organizations figure to migrate to contactless physical access control systems that

could be cloud-based, how do security measures work in that environment?
Many companies that migrate workloads to the cloud still need to retain their security measures.

Companies can do this by investing in authentication and authorization tools. Identity and Access Management (IAM) tools are important in any business, but they require extra attention when dealing with the complexities of cloud security. Companies must evaluate how their data will be secured and accessed from on-premises into the cloud. To secure these accounts, user identity and access management tools to set up identity federation and also multi-factored authentication.

Companies need to streamline efficiencies with single sign-on identity and access management tools - especially if their respective work environment uses multiple cloud and on-premises accounts. Through a single sign-on identity and access management tool companies can increase employee and IT efficiencies, improve security capabilities, reduce password management fatigue and streamline the user experience - enhancing security in the cloud and on-premise.