On Your Own in the Cloud?

Plan ahead to manage the risks of making the move.

By Ryan Gratias

The Challenge

We've noticed a trend as a growing number of organizations migrate to the cloud. Many assume the risks are similar to their internal data centers—nothing new to worry about. Others assume their cloud service providers will take on whatever risks are uniquely associated with the cloud. So it can come as a costly and time-consuming surprise when organizations not only discover new risks in the cloud, but also find they're responsible for managing and mitigating them.

To complicate matters, the cloudscape is in continuous flux as risks and compliance demands evolve. Regulations are increasing, including SOX (U.S. Congress's Sarbanes-Oxley Act), PII (Personally Identifiable Information), PCI (Payment Card Industry), and the European Union's recent GDPR (General Data Protection Regulation). Threat actors expose businesses to ever-evolving dangers, including data breaches (think Equifax) and cryptojacking (think Tesla).

Point B's Perspective

Point B helps organizations think early and differently about the security and compliance risks of moving to the cloud. Organizations that consider and address these risks in their cloud strategy are better equipped to make a successful migration. Creating a safe and compliant cloud infrastructure is a challenging task, but it's far easier to achieve up front than it is to retrofit and remediate later on.

If your organization is thinking about migrating to the cloud, now's the time to look at the security and compliance issues unique to the environment. Whether you're at the start of your planning process, or somewhere in the middle, Point B can help you assess and address your risks to ensure a safer and more efficient migration.

Cloud vs data center: secure your data's new home.

The cloud presents security and compliance issues that you need to know about as you plan your migration.

With data centers, security and controls are fortress-like, with a centralized infrastructure and specific entry and exit points. You manage the perimeters to ensure that everything inside can be safe and trusted.

The cloud, on the other hand, is comprised of a group of independent services, with each group responsible for its connectivity, security and operations. For many non-infrastructure engineering teams, this will be a new responsibility and worse yet, these teams may not even realize it is their responsibility in the first place. Fast-moving teams can easily put their organization and their customer's data at risk if the correct controls, training, and monitoring are not in place.

Data security is not the only consideration; costs must be controlled differently, too. Cloud scalability means that both internal employees and external threat actors, can spin up unlimited amounts of compute or storage at

significant costs. This differs from data centers, where users are physically constrained by the number of machines available for use.

Just as the risks differ, so do the approaches to mitigation. Applying the same methods in the cloud as you would in a data center will limit the value and flexibility you hoped to gain from the cloud—eroding the reasons for migrating in the first place. New risks call for new methods.

No one can identify the risks better than your people.

There is no "one size fits all" set of methods to manage risks in the cloud. The risks are unique to each environment and use case.

When your organization has a specific use case, your people can build controls around it. Develop your own cloud control framework based on those identified security risks. Consider current applicable regulations as you do—including SOX, PCI, PII and GDPR. For guidance, look at previous risk models and at best practices on cloud risks.

Be alert to control overlap when developing your framework to avoid multiple controls addressing the same risk. Leverage your cloud service provider and internal risk/security experts to mitigate these risks as part of your overall migration plan.

Finally, never underestimate the value of identifying your risks, or the time it will take to do it right.

Controls are not inherent to the cloud.

Cloud service providers, such as Amazon Web Services, Microsoft Azure and Google Cloud, take a "building blocks" approach by providing tools that can help you gain compliance in the cloud, but they do not manage compliance directly. Furthermore, the same cloud service providers make it exceedingly simple for individual teams to begin their migrations independent from the organization.

For instance, we've seen teams independently move applications and data to the cloud using personal credit cards, under the assumption that it is as secure as it was with the data center. That, in some cases, has unknowingly allowed direct inbound access to migrated data, in a manner that could not otherwise be detected in a centralized method by IT.

As you start your migration, consider your teams, the progress they may have already made and their understanding of cloud risks. Ensure you have an effective method of communicating and reinforcing your cloud strategy as well as monitoring and enforcing compliance right from the start.

Cloud controls are evolving every day.

Cloud controls are rapidly evolving in response to the world around them. Today the big headline may be cryptojacking. Tomorrow, it will be something else. But most major issues never really go away; they just recede into the background as new ones emerge.

Regulatory compliance issues are also changing in response to demands on emerging issues. Auditors face a learning curve that may impact business as new technology shakes up their previous understanding of the world. And as data privacy regulation matures, the requirements are growing more arduous (PCI, GDPR).

Last, but not least, fierce competition drives cloud service providers in the race to offer continuous innovation and improvements, with a major focus on controls. Expect to see new solutions come up on a regular basis.

Plan on a new sort of vendor relationship.

Vendor relationships and engagement models will change significantly when you move to the cloud. How will your support organizations and processes need to change to work with them? Who's in control of what? Plan ahead and ask your security team what questions and expectations they have for cloud service providers. Pay close attention to matters of access, privacy and compliance.

The Bottom Line

Any major IT change comes with risks. In order to make a successful migration to the cloud, your organization needs to identify and address these risks early on. Plan ahead for your journey and you'll have a safer, smoother path to making the most of your new environment.

