DATA INTEGRITY:
AS CRUCIAL AS YOUR CASH FLOW

Shared Responsibility Model: Cloud Backup Products

Your Data, Your Responsibility

08 August 2023

Dear Valued Customer,

You are receiving this communication as you are currently a subscriber of cloud services or other hosted services from Smart Technology Centre (Pty) Ltd.

The cloud has revolutionized how businesses operate, allowing them to take advantage of its scalability and flexibility while reducing costs. However, protecting data remains a critical challenge, with 98% of businesses reporting a cloud data breach within 1.5 years[1], according to IDC research – highlighting the need for organizations to take additional measures to protect their data.

Cloud service providers understand the importance of safeguarding data and applications within their environment and have developed a Shared Responsibility Model (SRM). This model requires businesses to take ownership of securing their data and applications within the cloud environment. Yet only 13% of businesses understand their role in safeguarding data[2].

Using cloud services, whether that be from Smart Technology or from globalized cloud services provider such as Microsoft Azure, Amazon AWS, or Google Cloud Services – the data is and will always remain your responsibility. You are solely responsible for ensuring your data is adequately protected in a manner that supports you or your business's needs.

Cloud providers have different approaches to protecting data, which adds to the complexity, and businesses need to understand the specific details and nuances from provider to provider. They do not however price in the value and risk of your data as this is nearly impossible – this would require a complete business valuation, Profit &Loss forecasts, intellectual value etc. which would result in a retail price point that is simply not viable or practical, further to which would need to be onward risk insured. As the Cloud Service Provider does not participate in the running of your business, this must be driven by the Customer according to risk mitigation.

As such, Customers must develop a holistic data protection strategy to ensure they have the necessary controls to protect their data even when relying on native tools included by their provider. This post will explore what this model means for Customers and why it is essential to have a comprehensive data protection strategy across cloud and hybrid environments to use cloud services safely and securely.

SMART TECHNOLOGY CENTRE (PTY) LTD
+27 87 310 1751
info@smartonline.co.za
www.smartonline.co.za

Block 10, Townsend Office Park
1 Townsend Road
Bedfordview, 2008
LEVEL-TWO B-BBEE Contributor

Why Are Businesses Increasing Their Adoption of Cloud Computing?

The availability of cloud computing and cloud related services has extended the possibilities for businesses; having workloads, applications, and services running in the cloud or hybrid environments gives businesses greater flexibility, scalability, agility, and efficiency. In addition to these valuable benefits, having a wide variety of Software-as-a-Service (SaaS) applications delivered via the cloud enhances operations, optimizes resource utilization, and brings agility and efficiency to business in an ever-shrinking global economy. It is no surprise that most companies have already embraced the cloud or are actively transitioning workloads, with Gartner estimating that over 95% of new digital workloads will be deployed on cloud-native platforms by 2025[3].

Another key advantage that makes cloud computing so attractive is that it allows users to access data and applications quickly and easily without requiring advanced technical knowledge or expertise, even more so low with low code rapid build applications. This makes it easier for businesses to deploy applications and manage data in a shorter time– something that would otherwise require significant technical expertise or experience, cost, time with traditional IT environments, with increased TTV (Time to Value).

For these reasons, more companies are turning to cloud computing to manage their data and applications. The SRM ensures that both customers and providers understand what needs to be secured within the cloud environment so that companies can take full advantage of this technology safely and securely.

What Is the Shared Responsibility Model?

The Shared Responsibility Model (SRM) is a cloud security strategy that states that, while cloud providers are responsible for securing their service infrastructure, Customers are responsible for securing their data and applications within the cloud environment. This division of accountability is designed to ensure that both parties understand what needs to be secured and how it should be done. This model allows companies to use cloud services' scalability and flexibility while having faith in their provider's ability to maintain a secure infrastructure.

To use cloud services safely and securely, customers must understand their role in the SRM. This means developing a holistic data protection strategy that considers their provider's native tools and any additional security measures the customer might need to put in place. By doing so, customers can better protect their data from threats such as malicious attacks, unauthorized access, data leakage, and more.

What Are Cloud Providers Responsible For?

Cloud providers are responsible for the security and privacy of their cloud computing infrastructure, including physical security, data storage, network protection, host firewalls, access control, and software vulnerability patching – depending on the service the Customer

has subscribed to. They must also ensure that their services meet legal and regulatory compliance requirements. In addition to providing all these critical components of a secure cloud environment, they are also responsible for the operational integrity of their system, ensuring its availability, scalability, fault tolerance, performance optimization, cost management, and overall reliability.

Each provider supplies a detailed description of what falls under their cover. For example, in its simplest form, Amazon AWS states explicitly that they are "responsible for protecting the infrastructure that runs all of their services in the AWS Cloud."

Finally, cloud providers should be transparent with customers about how they are protecting their data and informing them of any latest changes or compliance updates that may affect their operations.

What Are Customers Responsible For?

Despite cloud data being subject to the same responsibilities as any on-premises computing system, many companies remain unaware of this fact. The Shared Responsibility Model outlines that customers are responsible for securing the data and applications within a cloud environment – yet research has found that only 39% of organizations are confident in their ability to do so effectively[4].

Ensuring these responsibilities are met requires implementing additional security measures such as backup and recovery, encryption, identity and access management, and monitoring.

Key Data Protection Considerations

A robust data protection strategy for all workloads is essential for the total visibility and security of hybrid cloud environments. With regular backups of all workloads, organizations can be better prepared to respond in case of data loss due to either a cybersecurity event or a natural disaster. Additionally, having data readily accessible enables IT teams to restore any lost workloads quickly and efficiently with minimal downtime.

Encryption is critical when protecting sensitive data, such as financial or personal information, from unauthorized access attempts from external sources and internal personnel who could misuse customer information. Still, only 17% of businesses are encrypting at least half of the sensitive data they store in the cloud5. Customers should ensure they have robust encryption protocols across their environment and regularly re-inspect and apply the latest available options.

Identity and Access Management (IAM) is also essential for cloud service customers. Implementing an IAM system will enable customers to control who has access to their cloud environment on a user level, allowing only authorized personnel to view or modify data. By utilizing multi-factor authentication, customers can enjoy better protection from breaches and limit the potential damage a malicious actor could cause. Additionally, customers should ensure that their authentication methods meet the standards set by their industry's governing

body or regulatory agencies. Furthermore, companies should have a Separation of Duty (SOD) policy to further protect cloud data from misuse by any single account holder.

Monitoring and Managing cloud and hybrid environments is a complex task, as cloud-based data resources constantly change. Therefore, using a monitoring and observability service is essential for administrators to ensure the security and proper management of cloud data. Cloud-native tools such as Amazon CloudWatch and Azure Monitor enable real-time monitoring and visibility into cloud, hybrid, and on-premises applications and infrastructure resources. The provision of data analysis not only helps administrators gain actionable insights from cloud data but also access crucial information about the performance of their cloud environment.

By following the best practices regarding security protocols, businesses can ensure they have the necessary controls to protect their data while taking full advantage of the benefits offered by cloud computing services. Ultimately, it is up to each company's circumstances when deciding what specific measures must be taken to keep sensitive information safe from external threats or unauthorized access.

Today

As a Smart Technology Customer, we understand that you rely on our services and expertise to store your data securely. While we take extensive measures to ensure the safety and integrity of your information when stored on our infrastructure, it is essential for you to take an active ownership role in data protection that works for you and your business, and no one knows your business better than you.

Regular Backup Verification - Where Customers have on premise data, it can and does occur that backup cycles are missed due to load shedding, or other events. Please ensure you are receiving back monitoring notifications inducting that status of your backups; if not please contact us to ensure the correct recipients are configured, this can also be done via your Veeam Cloud Connect login or Live Vault tenant login.

Make this a habit, of reviewing your backup report daily, or delegate it to a responsible resource, your data is as valuable as your bank statement - check it, your business depends on your data.

Multiple Storage Locations - Even though you have a Cloud Storage Service with Smart Technology, or even with another provider, there is no assurance or guarantee that unforeseen events may cause data loss, i.e., a terror attack be it physical or cyber, natural disaster etc. You only benefit from creating and storing your own copy, ensure these are stored off site across multiple devices, and be sure to encrypt them; diversifying storage options ensures additional protection against data loss.

Encryption and Security - Utilize encryption for sensitive data to add an extra layer of security to your backups. Make sure to store encryption keys securely. If you are not sure about this, please talk to us.

Test Restores - This is as important as ensuring your backup has cycle has run and the data is valid. Even though our systems perform a data validation and verification, which does not mean the data is usable and recoverable when needed. We understand that it is not possible to always restore all data due to its size, function etc. i.e., it is not possible to restore and evaluate entire Virtual Machines, this then would need to be in your businesses risk management framework and how your business would deal with a disaster.

Review and Update Backup Strategies - Regularly assess your backup strategies and adapt them as your data needs change for your business and compliance. You need to ensure that all essential files and data are included in your backup routine. If you have any questions or need guidance on setting up effective data backup strategies, please don't hesitate to reach out to our Customer Support Team (helpdesk@smartonline.co.za). We are here to assist you in safeguarding your data and preserving your peace of mind.

Manage Your Risk - Your Data, Your IT, Your Risk

We understand that Information Technology can be confusing and is even a grudge purchase, and it is just too easy to leave it to "IT" as it is all working 'fine'. However, in today's technology landscape, it is vital for Customers to understand your systems and data at an overview level, and more importantly to fully understand where risks may exist, and how these can be mitigated accordingly. Whist we as your provider can support you on this journey, risk mitigation and management remain a Customer driven function.

The best way to do this, is to simply assume and plan, that should all information systems in your organisation collapse or go offline, be it cloud or on premise, your business requires a detailed disaster recovery plan to ensure your key operations can function - be that manual or as related failovers. Too often when critical systems fail, Customers simply have no plan - IT is merely actor in the theatre, the orchestration thereof requires a detailed plan that is Customer driven and owned. Similarly, it is key to note that even where your IT support may be outsourced, typically this only covers 'break fix' support, and does not extend to risk management and related disaster planning, the risk responsibility remains with the Customer.

In today's digital economy, information systems can no longer be a grudge purchase, an afterthought, or worse an assumption. IT needs to be front and centre along with all other critical pillars in a healthy business - remove IT from your business and it will not function today.

The International Standards of Auditing 315 ("revised ISA 315 - Identifying and assessing the risk of Material Misstatement"), is also now effective for audits of financial statements for periods beginning on or after 15 December 2021, thus creating new audit requirements that speaks to technology as a separate reporting item.

The now outdated previous standards for auditing did not consider IT risks and controls as a critical aspect, and this should be viewed as a welcomed addition.

Further coupled with effective Critical Security Controls (CIS Controls) available, this being a set of prescriptive, prioritized, and simplified best practices that Business can now use to further strengthen their cybersecurity posture though individual control mechanisms.

In a digital world, avoiding this key variable could pose great risks for your business, and even potentially render it void - Data can be recaptured, but not recreated and neither can time.

Your Business, Your Data, Your IT, Your Risk.

Thank you for choosing Smart Technology Centre, we value your trust and are committed to providing you with exceptional service.

References

1.IDC survey, commissioned by Ermetic. – 2. ESG Research Report, The Evolution of Data Protection Cloud Strategies, May 2021 – 3. Gartner IT Symposium/Xpo 2021 – 4. CSA Understanding Cloud Data Security and Priorities 2022 – 5. 2021 Thales Global Cloud Security Study – 6. PWC Cyber Security Outlook 2023 – 7. BlueFort Security 2022 CISO survey – Help net security – 8. IBM and the Ponemon Institute's 2021 Cost of a Data Breach

SMART TECHNOLOGY CENTRE (PTY) LTD
+27 87 310 1751
info@smartonline.co.za
www.smartonline.co.za

Block 10, Townsend Office Park
1 Townsend Road
Bedfordview, 2008
LEVEL-TWO B-BBEE Contributor