Summary Insights: Preventing Cloud Data Exposures

RFG Perspective: There are three types of cloud data exposures that enterprises need to guard against: rogue or ungoverned shadow IT clouds; gaps created by hybrid multi-cloud inconsistencies; and the inability to stop unauthorized users or data from being copied, modified or stored. Data loss prevention (DLP) is, therefore, an important area for improving data-protection policies and gudelines throughout the organization.

However, the majority of cloud data protections put into practice to secure information tend to be inadequate or out-of-date, or both. This situation leaves sensitive enterprise data, proprietary data and personally identifiable information (PII) data at risk when it moves into public clouds.

Unfortunately, hackers only need to find one opening in the overall data-protection regime in order to extract or damage the targeted data. For this reason, IT organizations must keep current with the best data-protection practices – and must put measures in place to ensure that the blast radius of any breach is minimized.

INTRODUCTION

A careful examination of business executive views and practices as they relate to cloud migrations of enterprise data shows that there is often a limited understanding of the data protection requirements and guardrails.

While business is shifting to the new digital economy, the culture around data protection has not undergone a similar change. The result: many people are not cognizant of the full range of data exposures created by shifting applications and data to the cloud.

However, for the most part, IT executives realize that clouds represent a greater attack surface than traditional data-center environments, which have many built-in data safeguards and practices. That's why new guardrails are needed to minimize risks affecting enterprise data – including data-at-rest and data-in-transit -- in the era of cloud migration.

Nonetheless, IT has often fallen short in its implementation of identity and access management (IAM) tools and controls, compared with computing environments centered around data-center "core" operations. Additionally, IT has moved data from legacy environments and created new databases that may not provide all the proper data discovery, tagging, classification and labeling technologies needed to protect end-users.

It is imperative that business and IT executives make senior corporate management and the Board of Directors aware of their cloud data risks, which threaten the

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

company's risk posture. It's also vital that they obtain funding to address key data risks that could materially impact the enterprise. These risk exposures and corrective initiatives need to be addressed monthly – or, at a minimum, quarterly.

RFG 100 Panelists and Insights from Participating RFG 100 Executives

On June 30, 2021, Robert Frances Group facilitated an RFG 100 videoconference entitled: "*Preventing Cloud Data Exposures."* This video conference examined what processes are required for the development and maintenance of a quality data loss prevention (DLP) program.

The panelists on the call were:

- Kim Lancaster, Head of Data Privacy and Security, Mango Languages
- Rich Isenberg, Partner, McKinsey & Company
- Yair Frankel, Next Generation Security Executive, BNY Mellon
- Vishal Gupta, CEO, Seclore

POLL RESULTS

Prior to the June 30, 2021 video conference, RFG 100 executives were polled about their biggest cloud data exposure challenges. We found the following results in the polling data for this group:

- The top business challenges to cloud data exposure are: imprecise requirements; lack of control of cloud environments; inability to control data access, modification or movement; and cultural and process issues.
- The top IT technical challenges are: lack of consistency and proper guardrails; identity and access management (IAM) software and associated controls; and data management processes and controls.

When thinking about architecting for clouds, one either designs for a compute cloud or a data cloud.

For many major financial companies, when they think of "cloud first," the directive is aimed primarily at compute and storage resources. In general, stateful data was marked to remain in the data center – and not on the Cloud. This disjointed strategy created compliance, implementation, privacy, resiliency, and security problems.

Often, the speed-to-market approach that was executed by the lines of business resulted in application affinity, data gravity, and security/compliance inconsistencies in the workloads that were moved to the cloud.

Now, we are in the second great wave of cloud migrations – one which will bring many more enterprise workloads – even in the financial world – to the cloud, or the hybrid cloud (spanning on-prem and off-prem data processing).

In this wave, cloud-native applications are being adopted to run alongside traditional, transaction-based applications, creating a mixed environment on the cloud. Many organizations counter this mixed environment by adopting containers, Kubernetes and Kafka. But deploying both types of applications – cloud-native and traditional – on the cloud may not be enough. Now is the time to focus on protecting enterprise data in this New Normal cloud

RFG believes that IT management, along with senior corporate management and corporate boards, did not fully realize the implications of their initial actions in the first wave of cloud migration (2008-2019). It was not until individuals throughout the enterprise gained sufficient knowledge of their new cloud environments that they became more aware of their firm's data exposures and of their firm's need to become compliant across the global landscape.

Presenting to the Board

One should always assume that members of the Board of Directors do not have a complete and comprehensive view of the different cloud environments and of the types of data exposures associated with them. Therefore, when presenting to the Board, it is best to present the data priorities and risks in business terms and the associated ROI for those solutions.

RFG believes it is best to unify all the audit, compliance, risk, and security concerns and projects into a discussion of a combined compliance suite – and to address it as a business opportunity.

Compliance is often viewed as a cost of business – and not as a revenue opportunity. However, when presented appropriately, compliance with data policies can be framed as helping sales and marketing discuss the firm's application advantages. Among these advantages are minimizing customer compliance, security, and risk exposure. The biggest challenge with this approach is getting the various teams inside the company – across business units – to collaborate, to create and to support a common policy for data-loss-prevention (DLP).

It's best to show the advantages of what is being proposed. This form of presentation and conversation will likely resonate with the Board of Directors rather than a technical presentation. Finally, one can aggregate the business advantages in terms of what one panelist called OPIs – opportunity indicators. OPIs are useful in presenting the future opportunities that are possible paths to business revenue than a compliance suite that is being added to bolster existing data-loss-protection efforts.

The Shared Responsibility Model

Regardless of what cloud service providers say, or some executives think, there is no such thing as a shared-responsibility model. The Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB) last March issued a memo on their view of the shared responsibility model for cloud service providers (CSPs).

Whether an enterprise's goal is a full migration to public cloud and exiting data centers, or moving to a future hybrid cloud, regulators are increasingly examining financial institutions to gauge the effectiveness and security of their cloud programs.

Importantly, regulators are making it clear that the banks and the financial firms are completely accountable for having full visibility and for managing the monitoring and testing of all risks associated with cloud-based operations. The conclusion of the joint OCC and FTB memo is that these regulatory institutions do not believe there is a shared responsibility model. The March 2021 memo underscores their view that all accountability and responsibility rests with the enterprise.

Data privacy

Enterprises should not think of the cloud as a new environment to address; rather, they should view it as an extension of their environment. Whatever controls and data privacy actions are required for legacy environments must be extended to the clouds – and enhanced as clouds pose a greater attack surface.

That expanded attack surface is created with each cloud provider offering different controls, guardrails, privacy, and security characteristics. In addition, various CSPs may make changes to their tools faster than the enterprise's governance processes can move to regulate them.

Enterprises need to be aware of data being exported from, or imported to, the cloud because it is easy to lose control of data as it gets copied, replicated or transferred to other systems. This includes systems owned by business partners, systems in the supply chain, or end-users' personal devices. Plus, there is no mechanism that provides linkage between a cloud service breach and an enterprise data breach.

To ensure end-to-end data security, corporations must make sure that data that is traveling through the cloud is carries its own security, privacy, geofencing, and compliance policies. In this way, the corporation's data policies will get embedded into the data when it is stored or archived. With this approach, no matter where the data goes, the controls go with it. Otherwise, IT will be struggling to protect the data, even when it resides on somebody else's computer, in somebody else's application, or when it is in transit in somebody else's network.

One of the newer technologies that is emerging is data-centric security platforms. These are platforms for providing a centralized view of the data. They not only address discovery of where data is, but they also extend to classifying the data, to protecting the data and to doing data centric audits.

These centralized platforms provide two functions: to keep the data compliant and to prove the data is compliant. Some of them will integrate with the discovery capability of a cloud access security broker (CASB) or a DLP system that will provide a classification capability via automated classification tools with the rights and encryption tools built in. Some of these platforms handle rights management for unstructured data, as well.

GDPR and CCPA Are Evolving

Some other factors to note, regarding the evolving regulatory environment affecting data protection and DLP:

- A lot of uncertainty exists today relative to both regulations. In the wake of the July 2020 Schrems 2 decision, the rules governing personal data transfers between the EU under its GDPR directives and U.S. have been invalidated. It is unclear how one can move data securely through one's systems between the geographies. In addition, how one handles data and its life cycle is unclear as the California consumer privacy act (CCPA) and similar pending state regulations are still undergoing iteration.

- Another struggle for the banks is open API banking that the EU is now enforcing. The U.S. has followed suit, promulgating its own APIs. Surrounding this discussion, it is clear that both entities are trying to attract third-party development communities around their open-source offerings so that new services will be available to existing banking customers.

- In addition, the FinTech companies are developing these offerings with decomposable services and microservices that integrate without any need

for human intervention. These new services create additional GDPR and CCPA challenges for IT organizations.

Things for business executives to consider in this ever-changing world of data-protection regulations: What, for example, is the GDPR impact as it relates to giving the customer notification when their data is shared and accessed in that model? How does an enterprise loop back around to address the GDPR "right to be forgotten" requirement for PII? Usually, there is no linkage and companies find themselves in regulatory trouble and facing potential fines when developing new applications because it is becoming increasingly difficult to comply with what they have built.

Encryption and Confidential Computing

Encrypting all of one's data-at-rest is not even close to being a solution for DLP. One would still need to deal with protecting data in transit and data-in-use. Furthermore, there is basic encryption – and there is application-level encryption – and both of these offer very different levels of data protection.

When an enterprise moves to the cloud, the application development team becomes responsible for data protection, because there are no standard patterns and technologies. Each group has developed its own processes and tools.

When some DevOps teams decide to encrypt the data-at-rest, they frequently leverage generic database encryption by taking advantage of the CSP's encryption tools, such as S3 tools. This level of encryption is often inadequate for data protection purposes because the service itself does the depiction transparently.

With this type of encryption, if an individual, such as a DBA, has access to databases, then he/she can get access to the data. And, if a configuration error is made, outside hackers may gain access. That is the way that Capital One data was breached back in 2019. The data was encrypted, but because the CSP had credentials, the service was decrypted.

To remedy this data-protection shortfall, what is really needed is application-level encryption or field-level encryption, which reduces the number of potential attack vectors. With application-level encryption, where the application itself is responsible for getting the encryption key, DBAs and development teams do not have access to the data. Rather, only the application itself has access to that data. With application-level encryption and field-level encryption, there is a higher level of data protection – and a greatly reduced number of attack vectors.

Another approach is to support fully homomorphic encryption, which allows applications to do a limited set of operations and processes on top of the data, even while the data is still being fully encrypted. This provides another layer of protection for PII data.

Many financial organizations and institutions are embracing confidential computing, which ensures end-to-end security and a set of private, custom "keys" that protect data, including data-in-use, from outside interference. Confidential computing creates a trusted execution environment for a set of applications along with the data, metadata and data dictionaries that are evoked and manipulated. It works by putting a wrapper around the execution environment, and one needs the keys required to access it.

Setting Policies and Objectives

When setting policies and defining objectives, the first step is defining the high-level principles for data protection. Then each of the principles should be divided into several objectives – and for each of the objectives, actual controls must be defined. Moreover, there should be data-owners that are accountable for each principle and control. Each principle/control has to be validated, verified and reported against.

Because this process is complex and there are a number of "gotchas," IT executives should take small steps when moving to the cloud. It does not mean that one needs to go slowly, but the first thing that built out should not be the one that carries the workloads that have the highest risk. IT executives need to know the answers to some basic questions:

- How do I consume them securely, in compliance with corporate and appropriate government regulations?
- How do I guarantee that the configuration is appropriate to be able to consume these services in a secure manner?
- How do I do that while meeting the requirements for enterprise data?
- How do I make sure that all the above complies with the corporate guardrails and checklists -- and that it does so with teeth?

Audit, compliance, and security teams need to work together to build the cloud suite of controls and requirements. As part of the effort, these teams need to be able to identify where data is at all times – in order to classify, tag and protect the data under all operational conditions.

RFG POV: The business units and functional leaders of audit, compliance, and security must work together to develop a comprehensive compliance suite that can be funded and monitored by the Board of Directors. A cross-enterprise cloud data governance board should also be created, so that the limits of data loss are addressed before business requirements are turned into code.

Unless there is buy-in from top management and a cross-enterprise cloud data governance board is implemented, cloud data gaps will continue to exist and be exploited.

Business and IT executives must be willing to commit serious resources to ensure that key corporate and PII data are properly protected at all times – especially when enterprise data is moved to the cloud. To ensure that these important cloud data practices are effectively established and maintained, senior corporate executives and the Board of Directors must understand the risks associated with cloud data usage – and remain involved with data loss prevention (DLP) policies.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*