CMSGu2015-06

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Cloud Business Applications

CERT-MU

National Computer Board
Mauritius

December 2015

Issue No. 6

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to give users an overview of the risks they need to consider when moving their business applications to the cloud and the security measures they need to take in order to secure these applications.

1.2 Audience

The target audience for this document include all organisations which are planning to move their traditional business applications to the cloud.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 provides a background on cloud apps.

Section 3 gives an insight on moving from a traditional application to a cloud-based one.

Section 4 presents some common risks of the cloud.

Section 5 explains how to mitigate the risks for your business applications in the cloud.

Section 6 concludes the document.

Section 7 contains a list of references that have been used in this document.

2.0 Background

Typical cloud apps offered by cloud providers include email, calendar, documents, online storage, sales, customer service, and more. Some of today's many cloud providers are well-known names in industry and include companies such as Amazon, Google, Microsoft, and Box. A selection of the top cloud apps in the market today include Cloud Drive, Google Apps for Business, Skype, SalesForce, Basecamp, Quickbase, and Box Business.

Using business apps in the cloud has widely recognized advantages: you save money by paying for only the IT computing resources you need, you can increase or decrease computing resources quickly without capital investment, and you can increase your reach to employees and users anywhere on the planet

3.0 Moving from a traditional application to a cloud-based one

Below are a few more necessary steps to take before deciding to move from a traditional app to a Web-based one.

1. Decide Why You Want Software-as-a-Service (SaaS)

Business agility, not cost savings, is the leading reason many companies are interested in cloud computing. SaaS is spreading quickly among business units and departments, not usually with the help or strategic guidance of IT to make sure the functionality isn't duplicated or conflicting with the company's other tools. SaaS allows you to access technology to respond to business demands in real time.

2. Think Architecture

Thoughtful architectural planning will help any organization in the long run, though it is becoming less necessary as SaaS providers begin to provide more ways to integrate SaaS and legacy applications, sometimes with another SaaS choice.

More than half the transactions on SalesForce.com come through APIs, meaning the software is programmatically connected to other systems, usually through manual integration work on the part of the customer.

SaaS providers like SalesForce are building much better integration into their apps, however. And third parties such as **Boomi** and recent IBM acquisition **CastIron**, can also help with two-way synchronization of data between on-premise and SaaS applications.

Third-party integrators such as **Appirio**, **ModelMetrics**, and **BlueWolf** also offer integrated sets of SaaS applications, sometimes selected by menu from a Web interface, sometimes built in custom engagements.

3. Take Inventory and Throw Out Apps

Few companies with significant IT infrastructures have total control over the number of applications they run. Maintaining duplicate applications costs more for everything IT touches storage, licensing, training and support. The problem is very common, and unlikely to go away.

About one quarter of most corporate apps contain critical data or functions that have to remain inside the firewall. The rest are generic or commoditized enough to be shifted outside or consolidated into a much smaller number of brands.

However, this is only the first step in matching internal and cloud-based apps. Back-office applications are good candidates for moving to SaaS, as are finance, HR and accounting apps.

4. Check More Than a Provider's Books

In SaaS relationships it is critical to know if a software provider is financially stable, well managed and uses secure, well maintained data centers. Hence, it is important to do due diligence checks on a provider's financial health and ability to pass audits for privacy or financial-reporting regulations.

Managing a lot of SaaS applications from one management console is a huge task. So is identity management. If you have to go to different consoles for every administrative task and to create or change user information, and someone leaves the company, what happens to all that information in all those unconnected places?

5. Compare the Right Costs

On-premise software looks expensive because customers have to pay the bulk of the cost upfront or across the first three years they use it. After that the customer's financial interest is to keep what it has paid for until long after the cost is repaid. That means relying on aging software and missing out on potentially beneficial functions in newer versions.

SaaS applications look inexpensive because the subscription cost is far lower than the pay out of an acquisition, and they begin delivering useful functionality more quickly than it would take IT to spec, build and test an on-premise application.

Without a coherent strategy and set of criteria for success, however, it's impossible to know if a SaaS application is delivering real value.

Without good integration tools and the ability to use them, customers have to repeat the same cycle of evaluation, testing, deployment and management with each application, rather than streamlining that process with better process and management integration.

The real challenge with SaaS is that we must make sure that the platform on which the applications are deployed can connect them easily and the end result of many SaaS contracts is less confusion, greater efficiency and a better handle on practical aspects of the business.

4.0 Cloud Common Risks

- **You do not have total control.**

  When you purchase IT services from a cloud provider, you do not have complete control over the computing resources your business needs to operate. What happens if the cloud provider goes out of business or changes its services or prices? What if it has an outage?

- **You might get stuck with one supplier**

  Not all cloud providers are the same. Their platforms are different with different hardware, software, configurations, and settings. Therefore, abruptly changing from one supplier to another can be difficult, even if you use the same app. You might get stuck with one supplier, just as you might with internally deployed apps. Email is a great example. The migration of email from one vendor to another is likely to encounter problems with the conversion of mail formats and customizations, whether on the cloud or in house.

  An app, especially a customized one, may not behave the same or even work properly on another cloud. If you begin to have problems with a cloud provider, it can be a long process to disengage and begin a new relationship with another provider. Until there is more standardization across the cloud-provider industry, switching from one provider to another will be a complex endeavor

- **Your data is protected by someone else**

  When using a cloud provider, your data typically is housed and protected by the cloud provider. Although the provider may be more able to purchase the latest security software and support, it doesn't have the same motivation to protect your data as you do. Granted, their business is reliant on their ability to protect data, but do they run their business like you do?

  The risks to data expand beyond data being destroyed. Trade secrets can be lost or data may be frozen because of a subpoena or other government action. Trade secrets can be stolen when a malicious actor takes the encryption keys needed to access your data.

Let us say the cloud provider advertises that it provides encryption and encrypted backup services to protect your cloud data. On the surface, that seems fine, but these services may not be sufficient for every business. Many providers use common encryption keys

Many providers use common encryption keys. They control for both storage and backup of customer data, which means that the malicious actor must only infiltrate the cloud provider to gain access to the data.

To complicate matters, your cloud provider is likely to be located far from your business physically. It is probably located across state lines or even in other (and multiple) countries. The locations of these data centers have legal implications. If your data is involved in a criminal case, the laws of the country and state where the data center is located dictate what the government can control. Your business data could be taken hostage even though you are not at fault. Further, many countries have stricter laws when it comes to encryption. A country may not allow data to enter or exit the country if it is encrypted using certain encryption techniques.

Therefore, performance benefits of internationally available data may require a tradeoff of lesser encryption to not violate laws in the country where the data center resides.

- **Your security is managed by someone else**

  Cloud providers are by design very large consolidators and aggregators of information in comparison to a typical corporate data center. In general, cloud providers have platforms that are more secure than your own or at least as good as yours because they have more resources than most (especially small) organizations to devote to security.

  However, since cloud providers house multiple customers' data on the same servers and they manage a much higher volume of data than even large organizations, they have the potential of being more desirable targets for cyber criminals.

  So even if we have not seen large attacks in the cloud much today, historically we have seen large companies with large security resources attacked. Those large

businesses understood their business needs and were tuned to their own business model. Can a cloud provider's security be tuned to every business model and workflow of all its customers?

- **You have to fight for information**

  Some of the largest cloud providers do not allow their customers to conduct inspections. Some cloud providers supply their customers with audit results such as a 3rd party SAS 70 type I and type II audits (or its replacement the SSAE 16) and various others. However, not all audits are equal.

5.0 Risk Mitigation for your business applications in the Cloud

- **Know what's already going on**

  Be sure you know what staff members in your organization are doing. Are they taking action without asking permission? For example, a project team may assume that it can use a cloud provider to quickly work on a proof of concept for a new tool. Or maybe the marketing department decides to purchase CRM services from a cloud provider instead of waiting months for a homegrown service. Staff can purchase these services easily by using a credit card or getting a free trial, unaware of the risks they are taking.

- **Be a smart consumer**

  Select suppliers who are willing to enter into agreements that enable you to operate your business effectively. In particular, make sure that the cloud provider's security controls are tuned to your business needs sufficiently. You may have an opportunity to negotiate a service level agreement (SLA) with a cloud provider, but more likely you will need to compare the SLAs of different providers and find the one that best defines the terms you need.

  Almost all cloud-provider SLAs have indemnification clauses that try to eliminate or isolate the cloud provider from responsibility or risk from loss to a business due to a service outage. Even if the terms limit risk and responsibility, it is in your best interest to negotiate those terms. If you do not have a contracts attorney on staff, a good time to find one is before signing with a cloud provider.

  You may not gain significant ground, but it is essential that you understand the terms and risks with each cloud provider to make an informed decision.

  If you can, negotiate contract terms that define your requirements for the computing resources, including security, data handling, and disaster recovery. Pay particular attention to your rights and obligations related to being notified of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement. Also make sure you understand where your data will physically be located and the laws that pertain to those locations, including who is considered to own the data.

- **Involve the right people in cloud decisions**

  Supplier selection, monitoring, and management are skills you must have to manage suppliers critical to your business. Find experts in your organization that understand supply-chain management. Involve both business leaders and IT professionals in making the decision about which cloud provider to select. As a business investigating a prospective cloud provider, it is critical that you read available audits and assess the reputation of the auditor as well.

- **Be cautious**

  Build trust with cloud providers slowly. Start by using the cloud provider for non-critical services and evaluate how well they meet your needs and avoid problems. Slowly build trust over time by extending what you use on the cloud little by little. Using this incremental approach buys time and opportunity to learn and make adjustments to the business relationship.

  Be selective about what you control and what you choose to be supported on the cloud. Keep your business-critical apps off the cloud, at least at first. If you can maintain control over data from the app, maintain that control. Compare the risks and benefits of keeping your apps and data on your systems vs. the risks and benefits of moving it to the cloud. Both choices have risks; consider them all to make a good decision. Select providers that have a mechanism for unique encryption keys per customer.

  This mechanism is intended to reduce the risk of unauthorized access to your data. Instead of being controlled by the cloud provider, these keys can be controlled by you or securely escrowed to ensure recoverability.

- **Monitor your cloud provider's activities**

  Find a way to ensure that the terms of the SLA are being honored. Keep abreast of the security controls used by the cloud provider and its ability to keep up with trends in cybercrime. Demand the information you need to monitor your business on the cloud. You should have access to the same information you would if the service was in your organization. Include terms in the SLA that ensure you have the right to receive the

information you need without resistance. Be as specific as possible to protect your access to critical information.

- **Plan for cloud outages**

  All cloud providers have outages. Amazon, Salesforce, and Microsoft are only three of the cloud providers that had outages in the last year. Ask the cloud provider about its disaster recovery plans and have a disaster recovery plan of your own that includes cloud apps.

  Investigate a hybrid approach in which you have a private cloud that works with a public cloud. You, or a paid cloud management service, manage your private cloud to scale to a public cloud as capacity is needed. Also consider a multi-public cloud implementation of a service across two or more cloud providers.

6.0 Conclusion

You can use cloud apps for your business; just be sure to fully understand the risks and how they might affect your particular business and industry. Be aware of how your staff may already be using the cloud, be a smart consumer of cloud services, involve people with the right skills in making cloud decisions, use an incremental approach to build trust slowly, monitor your cloud provider's activities, and plan for cloud outages. These activities will help you benefit from cloud service flexibility and cost savings while protecting your business.

7.0 References

- **https://www.us-cert.gov**
- **www.cio.com**
- **www.informationweek.com**