SALESFORCE SPECIAL

CIOReview

The Navigator for Enterprise Solutions

OCTOBER 29 - 2015 CIOREVIEW.COM

IN MY OPINION

Dr. J T Kostman,
Chief Data Officer,
Time, Inc.

CIO INSGIHTS

David W. Glenn,
Partner & CIO, CIO Consulting Services,
Tatum US

Salesforce:

Delivering a Futuristic Information System

Marc Benioff,
Chairman & CEO

CIO REVIEW
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

Security of Cloud Computing

By Anthony Scarola, CISSP, Director of Technical Information Security, TowneBank

Ugh, "cloud". The term and how it has been applied to hosted computing services is disappointing. Hosting providers have repurposed the cloud placeholder—typically used by network engineers to depict complex, yet understood technologies—to title their offerings. We now have many businesses buying into the technology without clearly understanding it or the risk behind it. Although cloud breaches are uncommon, [thus far], we have seen a number of availability-related attacks with significant downtime and business impact. Before moving to the cloud and incurring additional business risk, it would be wise to first understand the technology behind it, the threats, the risk, and work to implement effective security controls before becoming a statistic.

Cloud Primer and Responsibilities

The National Institute of Standards and Technology (NIST) defines cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Understanding the three 'service models'—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) is important. With IaaS, such as Amazon Web Services (AWS), the provider resells networking, storage, and virtual/physical servers; you are responsible for implementing and managing the operating systems, databases, and applications. With PaaS, like Google App Engine and Force.com, the provider installs and manages the OS and database, and you manage the application and data. And with SaaS, like Salesforce and Google Apps, the vendor installs and manages all the above and you and/or your customers manage the data.

Interim CIO at Norfolk State University, Andrea Di Fabio, worked to develop a terrific whitepaper available at vita.virginia.gov for the State of Virginia Agencies on cloud security considerations. Included are recommended security control areas and the party responsible for each, aligned with the three types of service models. This is a valuable resource to use when considering moving to a cloud provider.

Deployment Models

Clouds can be provisioned in one of four 'deployment models': private cloud, community cloud, public cloud, or hybrid cloud. It is imperative to understand each of these models and the differences in their security controls. Private clouds provide more controls for compliance purposes, such as for US-regulated industries, but typically at a higher price. As a vital part of your cloud vendor due-diligence process, ensure you clearly understand the deployment models, your options, and how they may impact your risk.

Cloud Threats, Business Impact, and Risk

Threats should be researched and discussed with potential cloud service providers at the onset of your due-diligence. Ask cloud vendors about possible and likely threats, and under NDA, include specific breaches they have endured. Potential cloud threats are numerous; many similar to those we already face to include system hacking, data loss or manipulation, and denial of service (DoS) attacks. Threats may come from external actors (criminal hackers, script-kiddies, hacktivists, organized criminal gangs, or even nation states), or insiders, generally all financially-motivated.

Jackson Schultz of GraVoc Associates states, “It’s not easy to ensure sensitive data you are sharing in the cloud is entirely detached from that of another of the cloud service providers’ customers”. There may also be privacy concerns considering the cloud provider may have full access to all stored data.

> **We have full responsibility to understand the technology, the threats, the risk, and apply adequate controls before flying to the cloud**

No computing environment is ever 100% secure; however, threats have different business impact due to potential risk. Actual business risk depends on the value of information/systems impacted. Clearly critical applications with significant customer data and high uptime requirements will have greater risk than others. Therefore, risk is commensurate to the value of information stored or processed, and relative to the business as it considers potential losses to the confidentiality, integrity, or availability of that information.

Securing Cloud Environments

The NIST Cyber Security Framework (CSF) outlines five operations to secure information: identify, protect, detect, respond, and recover. This process works well for protecting most information system environments including cloud-hosted. Identify means to understand, classify, categorize, and assign value to the information. This process assists with the understanding of your risk tolerance and in selecting and implementing suitable controls commensurate to the risk in order to adequately protect the data. Without this step, the remaining steps, to include the selection and implementation of security controls, may be a very challenging and expensive exercise!

Next, perform a risk assessment: ascertain potential threats, attack probability, impact, and inherent risk (risk before applying controls). Identify this risk by considering the impact of any potential adverse actions against the data, such as unauthorized access (confidentiality threats), undesirable modifications (data integrity threats), or system degradation (availability threats). Identify this risk up front so that you and your cloud computing vendors can work to adequately protect your information as you require.

Select and Implement Controls

Once inherent risk is realized, implement controls to protect each of three potential threat vectors (confidentiality, integrity, and availability), commensurate to your risk tolerance. Cloud providers will have many best-practice controls in place, or for purchase), [or optional, for you to buy] for protecting your information, to include two-factor authentication (2FA), IP address white listing, data encryption, data segregation, user access auditing, and policies/procedures. Check out NIST SP 800-144 for additional guidance. Besides preventative controls (e.g., firewalls, Intrusion Prevention Systems, and armed security guards), implement detection controls to monitor and alert on intrusions, availability issues, and unauthorized data manipulation. Last, considering the final two functions outlined by the NIST CSF (respond and recover), ensure sound, tested, policies and procedures are in place for responding to and recovering from any such incidents.

Summary

As keepers of our customer’s sensitive information, we have full responsibility to understand the technology, the threats, the risk, and applying adequate controls before flying to the cloud. Due-diligence begins with consideration given to the five functions of the NIST CSF, and researching potential threats against confidentiality, integrity, and availability. Perform a risk assessment to identify inherent risk, security control gaps. Identify and discuss control options with vendors. Perform these steps at a minimum and you will be well-underway to better plan for and mitigate breach risk in advance, when [not if] an attack occurs. If you determine that the security controls are not adequate and the risk of a cloud computing environment are too great to accept, you have options: limit the data hosted, implement ‘private cloud’, or even ‘no cloud’. Whatever you do, take your time, be diligent, research, assess, and implement your data environment securely. Remember, your customer’s sensitive information and your company’s reputation is at stake! CR

Anthony Scarola