Cloud Computing in a Restaurant Environment

How Restaurants Leverage New Cloud Computing Technologies to Achieve PCI Compliance

By Bradley K. Cyprus - Chief of Security and Compliance, Netsurion

Ever since the five major credit card brands (Visa, MasterCard, American Express, Discover and JCB), came together in 2004 to create the Payment Card Industry Data Security Standard (PCI DSS), businesses have been scrambling to make their organizations compliant. Sometimes, a new technology comes along which does not fit cleanly into the standard, making compliance an even greater challenge. Restaurant groups implementing Cloud Computing are challenged to create a balance between meeting their performance objectives and complying with the PCI standard. This paper will attempt to discuss Cloud Computing in detail and list where Cloud Computing and PCI compliance are sometimes in conflict.

Cloud Computing In Its Most Basic Form

While there are more technical definitions used to describe it (one of best comes from the National Institute of Standards and Technology – NIST), Cloud Computing is basically the concept of using shared resources over a network, typically the Internet. In most cases, the word "Cloud" can actually be interchanged with "Internet." So the real question is - How do you share computing resources over the Internet?

Based on current implementations, there are currently three common Cloud Computing service models that are recognized by NIST:

1. **Software as a Service (SaaS)** – using a remote third party application, usually deployed via a web browser or client software. At one time, this model was provided by companies that referred to themselves as Application Service Providers (ASP). A company that became famous for this model is Salesforce.com.

2. **Platform as a Service (PaaS)** – using a remote system for a specific service such as a database engine that runs centrally while the client software runs locally. Many ISP's offer a service called "SQL on Demand" that would meet this model.

3. **Infrastructure as a Service (Iaas) –** using remote systems as a whole for a broad range of network services. This usually entails a complete remote server or network such as file, Active Directory and e-mail. The remote clients will connect to the network over the Internet or other transport, but the actual computing power will be located off-site from the clients. An architecture that has been used for years that meets this description is Microsoft Terminal Services or Citrix Server.

As more niche markets open up and new network components are shared, the service models will change. Cloud Computing in many ways is still in its infancy, so these definitions need to be flexible enough to incorporate the new paradigms as they develop.

Cloud Computing Use In Restaurants Today

A primary advantage of cloud computing is central management. An IT department or third party service provider can make a single update to the Cloud, and without any further effort, that update will be in place for the entire organization utilizing the system. This benefit grows exponentially as an organization becomes larger because IT resources will primarily concentrate on the Cloud rather than being spread thin as they maintain multiple small networks.

Keeping in mind the three service models above, let's look at some practical examples of how companies can use the Cloud today:

Software as a Service (Offloading POS functionality to a web service) – When an entire POS software package is managed on the web, then a POS terminal becomes a simple computer with a web browser and an Internet connection. Functions such as user access, security, and daily reporting are centrally administered, and every location has the identical look and feel when the central system is maintained properly.

Platform as a Service (Running a centrally managed gift card database) - The gift card application integrates to the local POS software, but by housing the data centrally, every store (assuming a multi-unit chain) has access to the data simultaneously. Customers can access a web portal with real-time data that draws from a central information repository.

Infrastructure as a Service (A central Microsoft Terminal Server farm provides POS, back office, reporting, and data repository functionality) - In this case, a new store is set up from an IT perspective in a matter of minutes. Training is performed remotely, since users and trainers can view the same session from Terminal Servers. In a scenario such as this, the organization uses virtual servers so that no additional hardware is needed when a new server is deployed. A new server is created in the Cloud virtually, so it is possible to grow rapidly without requisitioning additional hardware. There are even third party service providers who rent the underlying architecture to the end user while maintaining the physical environment for a fee. This allows the restaurant group to have full control of its network without being burdened with much of the administrative hassle of maintaining a virtual server environment.

Cloud Computing Drawbacks

While central management is the primary benefit of Cloud computing, it is also a potential weakness. One isolated mistake can magnify in significance when it is reflected across multiple units.

Management of the Cloud is easier and less resource-intensive than traditional distributed networks, but critical mistakes can occur if it is not properly executed:

1. **Redundant Communication** – Remember that a restaurant will rely on offloaded services as part of Cloud Computing architecture. Therefore, it is critical to consider what will happen if the restaurant's primary communication channel fails. If the restaurant had implemented Software as a Service for its POS, then order taking, the kitchen system and customer checking outs will have to revert to a manual system. By having redundant communication, the restaurant will be able to stay online, allowing standard operations to continue.

2. **Formalized Testing and Approval Procedures for Every System Change** – Every organization should have procedures in place for making changes, but the importance of the process is directly proportional to the number of systems, or users, that will be impacted by a particular modification. Since every restaurant utilizes the same resources in the Cloud, making one wrong change could impact all of the locations negatively. For example, consider the impact if the price for a specific item is entered improperly. Every location will charge the incorrect amount because of this one mistake. Of course, when the price is corrected, every location will also be corrected simultaneously. Having a formal change and control procedure is not optional when cloud services are involved. Modifications must be approved by the correct stakeholders; testing a change in either a separate environment or after hours is crucial; and, most importantly, there must be a back out plan to revert the environment to avoid having a long-term issue.

3. **Cost** – While some Cloud Computing solutions will pay for themselves or even save money over time, there is frequently a large upfront cost for implementation. Also, an organization is faced with additional communication bandwidth costs associated with the increase in Internet traffic. A successful Cloud Computing implementation must include a complete cost analysis that takes into account not only the savings associated with centralized management, but the costs of the technology as well.

4. **The Cloud is not Always Appropriate** – Many people implement a Cloud Computing solution before understanding how much data must pass from the end users to the cloud. When a network connection is local, standard Ethernet connections to a server are fast and reliable. Data that moves from a restaurant to the Cloud potentially travels across the Internet at 1/100 of the speed of the local network. Depending on how much data is actually transmitted, the Cloud Computing solution may end up being too inefficient to be effective.

5. **Complex Security Concerns** – Each Cloud Computing model comes with numerous security challenges. As companies embrace one or more of the three cloud computing models, those security issues become more complicated to manage.

    - First, consider that each off-loaded service must be accessible by the remote locations that need to use it. This creates Internet security concerns for both outgoing traffic from the remote locations and incoming traffic at the Cloud site. In fact, many restaurant groups have determined that outsourcing their communication security with managed firewalls is the most efficient way to maintain adequate security in their environment without developing a cost-prohibitive infrastructure within their own company. A managed firewall solution, such as Netsurion's easily deployed Global Security Mesh™/VPN, enables companies to mitigate this risk without incurring unaffordable expenses.

    - Technologies, such as virtual servers, add additional security concerns into the mix. In a virtual environment, the underlying hardware systems host numerous virtual machines, so segmentation becomes a serious concern. Programs such as malware and remote management tools can cross supposedly segmented systems and compromise sensitive data by penetrating the virtualization layer. Since many organizations choose to use a third party to manage their Cloud computing needs for reasons of cost, efficiency, and expandability, it is important that any sensitive data stored in a virtual environment has enough security in place to mitigate the additional risk. From a compliance perspective (see below), validating security in the Cloud can be daunting enough to make a Cloud implementation impractical when sensitive data needs to be hosted.

The Cloud and PCI

Version 3.0 of the PCI Data Security Standard addresses Cloud Computing, particularly virtualization, more effectively than previous versions. This is most important for IaaS implementations. There is also a PCI Special Interest Group that generated an Information Supplement entitled, PCI DSS Virtulization Guidelines – June 2011 so that organizations will have an easier time adopting Cloud platforms. While this supplement does not change the PCI standard itself, it clarifies how to properly protect and segment virtual machines so that they will adhere to the existing PCI standard. To download the standard and other related virtualization documentation, visit *www.pcisecuritystandards.org.*

It is important to note that several requirements in the PCI Data Security Standard apply directly to Cloud Computing solutions (Exactly which requirements will vary based on the type of Cloud implementation). The following is a list of the requirements that are particularly relevant in a Cloud Computing environment:

- **1.1.(2-3) Current network diagram with all connections to cardholder data, including any wireless networks** – As certain parts of your processing are outsourced, it becomes more crucial to document the flow of cardholder data and verify the security associated with the third party Cloud solutions in place. Relying on a Service Level Agreement (SLA) is not sufficient for validation purposes.

- **2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.** – Using virtual technology means by definition that one physical server will be performing the function of multiple virtual servers. In any event, the standard demands that each virtual server is treated as a separate entity when it comes to which services it performs. This is the same separation that is demanded in non-virtualized environments. The point of this requirement is to minimize the cross-contamination of malware and rogue software by keeping services separate (either virtually or physically).

- **2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements** – Most Cloud Computing implementations will have a shared hosting provider. That provider must go through its own security evaluation, and it must provide the results to its clients. The documentation for this requirement appears later in the list.

- **8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two- factor authentication requires that two of the three authentication methods (see Req. 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.**
  - Since many Cloud Computing implementations incorporate remote communication, validating user access becomes a critical component from a security standpoint.

- **8.(5-8) Ensure proper user identification and authentication management for non-consumer users and administrators on all system components** – Since the Cloud is usually controlled in most cases by a third party, ensuring that the proper systems are in place can be a challenge. A collaborative effort must be made to ensure that the security is adequate because the third party is responsible to the restaurant group, not the end user. No one can alleviate the restaurant's responsibility to the end user, so proper due diligence is required to validate the environment where cardholder data is transmitted or stored.

- **9.(1-4) Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment** – Depending on what services are on the Cloud, it might be crucial to examine the physical protection of the systems as well. In Cloud Computing, the exact location of the data or exact path of the data may vary because of the nature of redundancy or server farms, so these particular requirements are more complicated than they might otherwise be. That does not eliminate the need for the examination. It only emphasizes why this set of requirements can be so challenging in the cloud.

- **12.8. (1-5) If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers** – Documenting how the service provider maintains the confidentiality of sensitive data and guarantees that confidentiality is crucial when dealing with Cloud Computing. Part of these requirements includes having a contract with every service provider such that they agree to maintain internal processes that are PCI compliant.

This list does not intend to claim that other components of PCI are not critical in a Cloud environment. Quite the contrary, every merchant who processes credit cards must comply with every relevant component of the PCI Data Security Standard at all times. The purpose of this list is merely to point out that some of the requirements actually become more challenging with Cloud Computing, therefore before implementing a solution, they should be considered.

Achieving a Balance

Cloud Computing is a compelling recipe for restaurants: The ability to centrally manage data and to rapidly create and deploy new capabilities, while paying only for the services used. Web hosting is a common entry point, and restaurants soon extend their use of the Cloud to test or develop new services, gather business intelligence, and run short-term projects.

Restaurants tapping into the Cloud are challenged to create a balance between meeting their performance objectives and maintaining compliance with the PCI standard. In fact, the Cloud is not always the ideal solution for every potential user. When contemplating a cloud solution make sure to ask:

- Is Cloud Computing suited to your organization?
- What measures should you take to avoid erroneous data entry, eliminate redundant communication, reduce upfront costs, and ensure highest levels of security?
- Will it lower your operational costs?
- How will you manage the security of your data in the cloud?
- Can you achieve PCI compliance within the Cloud?

The inherent complexities of Cloud Computing and PCI Compliance often command the resources and expertise of a specialist. Organizations such as Netsurion offer the expertise and solutions to guide your organization through the Cloud, enabling you to maximize benefits while avoiding potential pitfalls.

About Netsurion

Netsurion is a leading provider of cloud-managed IT security services that protect small- and medium-sized businesses' information, payment systems, and on-premise public and private Wi-Fi networks from data breaches and other risks posed by hackers. Netsurion's patented remote installation technology and PCI compliant cloud-based solutions simplify the implementation process and ongoing support. Any sized branch or remote office, franchise, or sole proprietor operation can use Netsurion without the costs of onsite support. The company serves the retail, hospitality, healthcare, legal, and insurance sectors.

7324 Southwest Freeway
Suite 1700, Arena Tower II
Houston, Texas 77074

P: 713.929.0200
F: 713.541.1065
Netsurion.com