CLOUD COMPUTING:
The Risks to the Retail & Hospitality Industries

March 2012

Sponsored by: AIG
Executive Summary

Cloud computing provides companies with the flexibility, efficiency, cost savings and adaptability to remain competitive in today’s rapidly changing global marketplace. The buzz around cloud computing continues to grow, but not all industries have embraced the technology with the same level of enthusiasm. For example, large multinational retail and hospitality companies continually look to improve service capabilities and cut expenses, but have been slow to jump on the cloud bandwagon.

Although the benefits of cloud technology are apparent, many companies within the retail and hospitality space are familiar with high profile data security breaches, and they widely consider these technological solutions to lack sufficient maturity for the market. They have concerns about the security and reliability a cloud solution can provide as a platform for facilitating PCI-compliant transactions. However, the competitive nature of both industries, coupled with the lure of reducing costs, improving efficiency and updating outdated legacy applications, are proving hard to ignore as some companies begin to explore opportunities in the cloud.

Introduction

While the phenomenon of cloud computing has shifted from conceptualization to implementation for more and more companies worldwide, the associated risks of cyber-attacks and data breaches have escalated almost as quickly. For example, a coordinated series of attacks by the hackers’ collective, Anonymous, recently disabled websites belonging to the United States Justice Department, the FBI, Universal Music Group, the Recording Industry Association of America, the Motion Picture Association
A recent attack on Sony Playstation, by hackers using Amazon’s Elastic Computer Cloud, a cloud computing service, as a platform, has further raised concerns about the security of cloud computing.

of America, and Broadcast Music, Inc., among others. The director of the National Security Agency recently warned that this same group within the next couple of years could have the ability to cause a targeted power outage through a cyber-attack. Groups believed to be affiliated with nation-states, allegedly including China, routinely launch so-called advanced persistent threats to access and steal information from government corporate websites. One ambitious American hacker and two associates were alleged to have been responsible for the theft of information on 130 million credit cards, primarily from large retail companies.

The recent surge in cyber-crime comes at a time when cloud computing is rapidly gaining popularity as a way to economically manage data storage and computer software. This has led many companies to question whether their information is safer “in the cloud” or on their own systems. With the average cost of a data breach rising for five years, and presently at $7.2 million per breach event and $214 per compromised record, making the proper decision has never been more important. This is especially true of companies in the retail and hospitality industries, which have been the targets of sophisticated cyber criminals in search of credit and debit card information. A recent attack on Sony Playstation, by hackers using Amazon’s Elastic Computer Cloud, a cloud computing service, as a platform, has further raised concerns about the security of cloud computing.

Concerns about cloud computing are further compounded by the need to comply with data security standards imposed by credit card companies. The Payment Card Industry Data Security Standard (PCI DSS) may be more difficult to fulfill using cloud computing. This could expose merchants not only to security vulnerabilities, but also to fines and penalties for failure to comply with standards. Additionally, cloud computing could create problems for companies that need to meet data security and privacy standards for customers outside their home country.

The Lure of the Cloud

Cloud computing is a new term for a variety of services that have been around for years. The “cloud” refers to delivering hosted services over the Internet on demand, from any location at any time. Services include data storage and retrieval, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud infrastructures come in three varieties: private, public or hybrid.

The Private Cloud is controlled by the entity itself and is designed for organizations that want more control over their data than they can get through third-party hosted services. Private clouds may be located across multiple locations owned by a single customer. They
Cloud computing offers businesses several benefits, including a long-term cost effective solution that can often be paid for incrementally, allowing organizations to budget appropriately and manage cash-flow.

are not shared with other customers or tenants, and may be the property of the entity or owned by a service provider.²

The Public Cloud is a solution whereby the service provider makes applications and storage available to the general public over the Internet. An organization utilizing these services does not own or have control over any of the system components. System components in the public cloud will vary depending on the type of service.³

The Hybrid Cloud is a combination of both public and private cloud infrastructures. For example, a company may store its archived data in the public cloud, while storing its customer data in-house on a private cloud. Hybrid clouds are ideal for companies looking to take advantage of cost savings and scalability provided by the public cloud while not exposing their most sensitive data to a third-party and their vulnerabilities.⁴

The size and scope of a business often determines the suitable cloud environment an organization should utilize. Because small to medium-sized companies rarely have the resources to manage and implement a proper security system, they tend to lean towards the public infrastructure option, while larger, multinational organizations lean toward private or hybrid environments. “Whether large or small, for retailers looking to slowly move operations into the cloud, the first step could be to place basic catalog information on the cloud, but use its own servers to process transactions,” said Tracie Grella, Global Head of Professional Liability at Chartis Insurance.

Cloud computing offers businesses several benefits, including a long-term cost effective solution that can often be paid for incrementally, allowing organizations to budget appropriately and manage cash-flow. The cloud also offers increased storage capacity and eliminates the need for IT departments to continually maintain current software. It provides increased flexibility and mobility, as the cloud can be accessed from anywhere in the world at anytime. Finally, it allows IT departments to shift their focus from updates and general computer hardware issues to mission-critical strategies such as innovation and efficiency.⁵

Retail & Hospitality Data Security Risks

The cloud offers clear benefits to retail and hospitality companies, but security concerns have deterred many larger organizations from making the leap to a cloud solution. Companies in these industries are especially sensitive to data security issues because of a number of recent high-profile cases and events.
In 2011, Epsilon, an email marketing services company that does business with many of the retail and hospitality giants, reported an extensive data breach event. The breach impacted anyone who ever signed up to receive a retail offer or alert through its email account. While email addresses may not be considered critical data, the concern was that thieves would use that information to conduct a phishing campaign in an attempt to lure people into releasing more valuable information. Companies affected included Ritz-Carlton Rewards, Marriott Rewards, Home Shopping Network, Walgreens, Brookstone, New York & Company, and Kroger among others.

In 2005 a data breach of the TJX Companies resulted in 45.6 million credit and debit card numbers being stolen over a period of 18 months. The breach occurred in the TJX computer systems that process and store information related to payment cards, checks and merchandise returned without receipts. In the United States and Puerto Rico customers of T.J. Maxx, Marshalls, Home Goods and A.J. Wright stores were affected, in addition to Canadian customers of Winners and Home Sense, and U.K. customers of T.K. Maxx brand stores. The incident cost the retailer more than $320 million.6

In a related case, entertainment company Dave and Busters, Inc. was charged by, and ultimately settled with, the Federal Trade Commission (FTC) for preventing the vulnerability of its' consumers' credit and debit card information to hackers, resulting in hundreds of thousands of dollars of fraudulent charges. The FTC alleged that Dave and Busters. Inc. failed to take the necessary steps to secure its customers personal information on its computer network. Consequently, a hacker installed unauthorized software and gained access to information about approximately 130,000 credit and debit cards.7

The commonality between the latter two high profile breaches is that they were both master-minded by the same individual. This individual was also charged with infiltrating computer networks of Heartland Payment Systems, 7-Eleven Inc, Hannaford Brothers and other national retailers. The federal government has deemed these cases as the largest collective incident of credit and debit card theft ever prosecuted in the United States, resulting in the theft of information about more than 130 million cards.

It may seem that hackers are solely targeting large companies since these are the events that make headlines, but they are also a significant threat to small businesses. In fact, Visa Inc. estimates that approximately 95 percent of its credit-card data breaches involve information about customers of its smallest businesses. Although they may not know it, smaller retailers are under constant malicious network attacks since they tend not to invest in IT resources, cardholder data monitoring, and preventative network security solutions. This was highlight-
Cloud vendors are increasingly driving security as a key selling point, but many larger retail and hospitality companies still question whether a cloud solution can truly do a better job of protecting their data.

ed in a survey by the National Retail Federation and First Data Corp. in 2010, focused on small and mid-size retailers. The survey found that 64 percent of respondents believed that their businesses were not vulnerable to credit card theft, and only 49 percent had reviewed their security safeguards.8

The cost of a data breach for a small business can prove catastrophic. The expense associated with investigation and remediation of the breach alone can be steep. If you add business interruption losses due to the inability to accept credit cards, lost business due to damaged reputation, and fees or penalties charged by the credit-card companies for failing to comply with PCI DSS, many small businesses may find that they have no choice but to file for bankruptcy.

The retail and hospitality sectors are prime targets for bad guys who prey on small and medium-sized businesses alike by taking advantage of their lack of data security know-how and resources. For small companies lacking sophisticated IT resources, the cloud solution could represent a more stable and secure place to store data and manage transactions. Cloud vendors are increasingly driving security as a key selling point, but many larger retail and hospitality companies still question whether a cloud solution can truly do a better job of protecting their data. Additionally, companies of all sizes are faced with the question of whether the cloud provides a secure and reliable platform for facilitating PCI-compliant transactions.

Cloud Computing and PCI Compliance

The PCI DSS (Payment Card Industry Data Security Standard) is a widely accepted set of policies and procedures developed to maximize security of credit, debit and cash card transactions, and protect cardholders against misuse of their personal information.9 PCI DSS is essential to both the retail and hospitality industries due to the volume of personal information collected in conducting business and performing transactions. It is a minimum standard created to protect consumers from companies who would otherwise have done nothing.

The PCI DSS policy contains twelve requirements that are grouped within six core principles. The principles include: building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, restricting physical access to cardholder data, regularly monitoring networks and security systems, and maintaining an information security policy.10 Complying with these principles can be a challenge for some business owners in the retail and hospitality sector, since they typically do not have the proper resources or technical expertise.
With the cloud representing an ever more attractive alternative for industries with significant PCI compliance exposures, cloud providers more frequently emphasize within their advertising campaigns that they are in compliance with PCI DSS. This includes some of the biggest players in the cloud realm, including Amazon and Verizon. In actuality, they have only been validated against specific PCI requirements.

It is nearly impossible for cloud customers to automatically inherit PCI compliance. Certain aspects of PCI cannot be achieved by the cloud service provider, and can only be achieved at the client level. For example, to be compliant with PCI DSS, a business is required to review their logs on a daily basis, an exercise that must be completed by the cloud client.\(^{11}\) The following list comprises inherent characteristics of cloud computing that present challenges for achieving PCI DSS according to the PCI Security Standards Council.\(^{12}\)

“The distributed architectures of cloud environments add layers to technology and complexity to the environment.”

“Public Cloud environments are designed to be public-facing, to allow access into the environment from anywhere on the Internet.”

“The infrastructure is by nature dynamic, and boundaries between tenant environments can be fluid.”

“The hosted entity has limited or no visibility into the underlying infrastructure and related security controls.”

“The hosted entity has limited or no oversight or control over cardholder data storage.”

“The hosted entity has no knowledge of “who” they are sharing resources with, or the potential risks their hosted neighbors may be introducing to the host system, data stores, or other resources shared across a multi-tenant environment.”

Continued compliance with PCI DSS can be burdensome with violations resulting in hefty fines, along with the increased risk of data theft, reputation damage, and loss of customers. In reviewing the service agreements of cloud vendors, it is important to confirm the scope of their PCI DSS compliance. PCI requirements not addressed by the cloud service provider should be identified and documented, because they will ultimately be the responsibility of the client.
Multinational and Franchising Issues

In addition to data security and compliance with PCI DSS, large multinationals in the retail and hospitality sectors are also required to comply with the data security and privacy laws of the countries where they conduct business. This requirement can impact an organization’s decision to move information into a cloud.

For example, the United States does not have a single comprehensive data privacy law, but instead relies on several laws that each contains provisions on privacy and data security. These laws focus on specific industries (i.e. healthcare), or specific populations (i.e. children), but do not provide a comprehensive privacy framework. In comparison, the European Union has developed a more comprehensive approach by passing of the Information Directive of 1995, and the Directive on Privacy and Electronic Communications in 2002. The EU privacy laws prohibit the transference of personal information from EU residents to countries that are deemed not to provide the same level of privacy security. The United States is considered to be one of those high-risk countries.

For multinationals contemplating cloud services, significant legal implications can drive concern. Unlike the traditional outsourcing relationship, whereby a company purchases storage capacity in a dedicated data center, the cloud is not restricted by specific location or geographical boundaries. Certain cloud platforms make it nearly impossible to identify the location of data at a specific point in time because it may be scattered and stored across several data centers located around the world. In this situation, a company can find itself in breach of EU laws if the data of EU residents is transferred to servers located in prohibited countries.

To avoid these potential legal pitfalls, multinationals need be sure they remain in compliance with the EU and other government privacy laws that pertain to trans-border data flow before making the decision to move information into the cloud. When negotiating cloud service contracts, these companies should understand, and be in agreement with, the cloud service provider regarding geographic location of the data center and jurisdictional limitations required under EU or other laws. As noted below, some cloud providers such as Amazon’s Web Service specifically address these privacy concerns in their standard customer agreement.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities.
The primary concern for a franchisor is a potential data breach at one of its franchise locations, which could consequently impact the entire brand, specifically from a reputational perspective.

You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.13

Additionally, for organizations in the retail and hospitality sectors that offer and support franchising opportunities, the utilization of cloud services can pose further concerns. These issues also can impact an organization’s decision to move data to the cloud.

The primary concern for a franchisor is a potential data breach at one of its franchise locations, which could consequently impact the entire brand, specifically from a reputational perspective. In a franchisor/franchisee relationship, the franchisor will typically carry insurance coverage, and franchisees individually will have their own policies. While the scope of protection may be determined by the franchisor, each franchisee may obtain that protection from a different insurance company. This can create potential complications determining how and which insurance policy would respond in the event of a breach that affects both franchisees and the franchisor. “The last thing a franchisor wants is to get into a bitter dispute with its franchisee over the cause of a data breach and argue over who is picking up the tab while the state breach notification clock is ticking,” said Grella.

Insuring the Cloud

A common mistake made by many organizations is the assumption that along with the transference of data to a third party vendor comes the transference of risk. In fact, most cloud computing vendor agreements traditionally have been modeled after technology or outsourcing agreements significantly limiting the vendor’s liability. This remains common today, including with three of the largest providers of cloud services – Amazon, Google and Microsoft – as is evident below in excerpts taken from each of their online service agreements:

Amazon: “Amazon has no liability for .... (D) any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data.”14

Google: “Customer will indemnify, defend, and hold harmless Google from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys’ fees) arising out of a third party claim: (i) regarding Customer Data...”15

Microsoft: “Microsoft will not be liable for any loss that you may incur as a result of someone else using your password or account, either with or without your knowledge. However, you could be held liable for losses incurred by Microsoft or another party due to someone else using your account or password.”16
A comprehensive privacy and data security insurance policy should provide coverage for both first and third party costs associated with a breach.

However, competition always benefits the consumer, and this is increasingly evident in the cloud realm. A growing number of cloud providers are now open to negotiating the terms of their service agreements, limiting the liability of their customers. A necessary first step for any retail or hospitality company is to completely understand the terms of the service agreement, and attempt to negotiate anything deemed unfavorable. A common feature of cloud computing contracts is a financial cap limiting liability to the amount of fees paid by the cloud customer under the contract, often limited to a specific time period. A cloud customer might be able to get the vendor to increase the cap. With enough negotiating clout, the customer also may be able to have certain types of damages, such as loss of data, removed from the exclusions. A vendor may be agreeable to take on additional liability if they are offered a higher price for the service provided.17

Even if a vendor is unwilling to assume additional liability, the contract should outline the vendor’s obligations in the event of a breach. At a minimum, the contract should include a requirement to notify the customer of a data breach within a specified timeframe, and to provide pertinent details. Additionally, the vendor should be required to describe corrective actions and plans to prevent future breaches.18

In addition to negotiating favorable cloud terms and conditions, insurance also plays an important role for companies seeking peace of mind against cloud computing data security, privacy and business interruption risks. Traditional business insurance policies (i.e. CGL, D&O, E&O) typically will not respond to these risks, and instead often require a policy specifically developed to protect against privacy and data security threats. A comprehensive privacy and data security insurance policy should provide coverage for both first and third party costs associated with a breach.

Additional important coverage considerations for retail and hospitality companies include:

“A broad definition of “covered information,” including not only the personal and private information of individuals but confidential corporate data;

Coverage for legal liability damages and defense costs, as well as regulatory actions, fines and penalties (as permissible by law); and

Coverage for the myriad costs a company will incur to manage an incident.”19

Coverage for PCI fines or penalties

Breach notification coverage in states that do not have breach notification laws
But even the most secure cloud vendors may not be fully compliant with PCI DSS standards or the privacy and data security laws in some countries.

Since many retail and hospitality companies deal with customers outside their home countries, and since cloud services often span national borders, international experience and presence can be an important consideration when choosing an insurance carrier.

Conclusion

The stakes are high when it comes to data security and privacy in the retail and hospitality sector. For industries that have historically relied on cameras and mirrors to prevent the theft of money and information, coming to grips with the risks associated with evolving technologies, such as cloud computing, can be daunting. However, the benefits of cloud computing are compelling, and many companies have concluded that not only are the risks manageable, the cloud may even provide a safer environment for storing information, managing transactions, and conducting business.

But even the most secure cloud vendors may not be fully compliant with PCI DSS standards or the privacy and data security laws in some countries. Retail and hospitality companies should take precautionary measures to assure compliance, which, in the case of PCI DSS, often means that they will need to maintain an active role in meeting requirements. Additionally, companies should ensure that they are financially protected from the consequences of a data breach. They may be able to contractually transfer some of the risk to cloud vendors, albeit limited. To ensure adequate protection, management should speak with a knowledgeable broker about the benefits of specialized insurance coverage to mitigate the growing exposures associated with cloud computing.

This Special Report was written by Josh Bradford, Associate Editor, Advisen Ltd. and sponsored by Chartis Inc.