CASE STUDY

STOREWORKS

PCI COMPLIANCE REACHES FOR THE "CLOUD"

Major salon retailer adheres to Payment Card Industry Data Security Standard with the help of an innovative solution based on cloud computing and a robust payment processing platform.

Retailers may feel like they are playing beat the clock when it comes to remediating systems to meet ever-changing PCI DSS compliance mandates, however they cannot lose their focus when protecting sensitive, mission critical customer data. By using a scalable, end-to-end PCI-compliant payment solution, one of the industry's largest salon companies is streamlining its point-of-sale payment processing, keeping all of this sensitive data protected and still adhering to all compliance mandates.

Just uttering the words "data breach" is enough to make any retail chain's CIO shiver. In simplest terms, PCI DSS compliance is an industry-mandated security standard that requires all businesses that handle, process or store credit cards to take stringent measures to safely manage all sensitive customer credit card information, such as the cardholder's name, credit card number and expiration date. There are 12 core requirements and roughly 250 controls that must be followed to meet PCI DSS compliance.

For those companies that fail to comply, consequences are far-reaching. Embarrassment and brand-damaging publicity aside, breached non compliant retailers have already learned the hard way that PCI-related fines could reach up to $500,000 per incident.

As a result, merchants are hard-pressed to stay on top of newly created amendments and requirements. Besides monitoring potential exposure points, retailers must be equally mindful of protecting customer data that flows from their POS through various touch points across the company - all a breeding ground for a potential breach if not protected correctly.

That however, is only the tip of the proverbial iceberg. Once all weak spots are pinpointed, attention must then focus on how to protect and secure all network connections that link data into and out of these touch points.

"There is a growing misconception in the industry that if a retailer is PCI-compliant, then it also has a secure network," reports Anil Konkimalla, chief architect for STOREWORKS Technologies, an integrator and single source provider of store-level peripheral solutions, based in Minneapolis, Minn. "Retailers must wake up to the reality that recent publicized breaches involved reputable companies that were 'PCI compliant.'"

Retailers are even more vulnerable to attacks when they are working on antiquated, customized equipment. This was the exact case for one of the country's leading salon retailers - and operating 10,000 stores worldwide only intensified the problem.

WORKING IT OUT

Supporting a legacy Windows NT 4.0 operating system and homegrown POS software, the chain was also saddled with an unprotected dial-up network that authorized credit card payments. Credit cards were swiped on the POS terminal keyboard and passed "in the clear" over the insecure dial-upconnection. Besides being an invitation for even the most inexperienced hacker, the configuration certainly was not up to snuff to meet mandated PCI compliances. Both issues put the company at risk for data security breaches, and hefty fines from the Federal Trade Commission.

Eager to get its network and operations PCI compliant, the chain began investigating how to achieve all of the traditionally prescribed PCI remediations required for its legacy POS system, including Event Logging, Username/ Password management to create an audit trail of internal transactions, Anti-virus software and security patch updates. When the chain began investigating its options, it quickly learned that making even these rudimentary remediations could cost the company "millions of dollars," says Troy Stelzer, President of STOREWORKS.

"There is a prohibitive cost associated with getting legacy POS systems compliant using a series of patches, and then there is additional work that is required to get a 15-year old operating system and customized software compliant," he adds.

That was when the salon company approached STOREWORKS in hopes of finding another solution. STOREWORKS' technical team collaborated with the retailer and its Qualified Security Assessor to develop a robust, long-term solution. Besides wanting a payment-processing solution that met all required mandates, the chain also had a few of its own requirements.

It was ready to transition to a more efficient payment processing operation, one that had the flexibility to process a variety of electronic payment options, such as credit, debit, as well as gift cards. It also demanded a cost-efficient solution so it could keep its operating expenses low - especially at a time when the recession continues to take a toll on all segments of the retail industry.

Keeping all of the chain's pre-requisites in mind, STOREWORKS scoured the industry for the best option. After conducting a painstaking marketplace evaluation and testing several competing solutions, STOREWORKS recommended a combination of best-of-breed hardware, software and services that would become the industry's first firewall-protected payment gateway solution driven by a multi-lane payment device. This ideal solution is based on a three-pronged approach that not only meets these parameters, but also provides a seamless end-to-end solution.

7300 Washington Ave S
Eden Prairie, MN 55344
866.388.9990
STOREWORKS.com

The first step was to transition to a software-as-a-service plug-and-play payment processing solution. With a business model that requires retailers to pay a fixed monthly cost instead of costly per-transaction fees, SaaS options have grown in popularity during the ongoing recession.

This solution, called whizPay, from TalentBeat, Boston, Mass., is comprised of a listener module that reacts to activities on the payment device. Similar to a sniffer that monitors and analyzes network traffic, whizPay is a centralized one-way gateway that encrypts sensitive payment information and customer data flowing into the chain's MX880 payment device from San Jose, Calif.-based VeriFone Systems.

MX880 Payment Device

While this may sound commonplace, this solution further protects the chain by pushing the POS completely "out of scope" for PCI. Rather than plug the device directly into the POS unit, instead it is connected directly via Ethernet cable to a port on a stateful firewall switch. With the POS out of scope from a PCI perspective, the chain is no longer required to manage Windows updates, passwords or virus protection on the POS hardware or associated POS software.

As a shopper swipes their payment card on the VeriFone payment terminal, the whizPay platform transfers the data to whizPay's dedicated gateway, also provided by TalentBeat, which exists virtually in the "cloud." whizPay electronically connects to this distributed, virtual computing configuration, which processes and authorizes payments on-demand. Authorized payments are swiftly transmitted back to the payment terminal in a tokenized format, which tenders the sale.

Unique among gateway solutions, whizPay can also pull up a transaction to process a return simply by swiping thecustomer's credit card on the payment device.

Needing nothing more than an Ethernet connection and computer (or in this case, a peripheral device) to process transactions, retailers can manage as much or as little volume at any given time. Since the service is fully managed by the provider, in this case, TalentBeat, the retailer's operational costs remain low.

"Since all processing is transmitted through the whizPay secure gateway and handled in the cloud, and data is never stored or processed in the POS unit or payment device, the POS' terminal and operational software stay out of scope, so to speak, and the retailer is able to eliminate two very crucial exposure points while safely complying with PCI standards and mandates," Stelzer explains. "Processing payments via an Ethernet connection takes security to the next level and also saves a significant amount of time per transaction."

REWARDING LOYALTY

Equipped with a new way to protect sensitive customer information, the salon is currently planning how to leverage its new payment infrastructure's marketing platform to build customer loyalty and grow sales. Architected to take advantage of the intelligence captured in each transaction, whizPay enables merchants to use customer data garnered during payment transactions and apply details to personalized customer engagement programs.

"The modular structure of whizPay enables retailers to add capabilities as their needs change," stated John Moran, vice president of sales, TalentBeat.

Similar to its payments transactions, whizPay pulls loyalty information into a database residing in the cloud. After polling shopper details on-demand, and analyzing customer purchase patterns, the chain can create personalized graphics and messages intended for individual shoppers. Then the cloud-based gateway transmits all marketing collateral for display on the VeriFone payment device, however all data is stored virtually.

The solution is so robust, it will also allow the company to deliver different messages to shoppers visiting different areas of the salon. "For example, a shopper tendering a sale at the hair salon may get a different message than a shopper settling her bill in the shop's spa," says STOREWORKS' Stelzer.

The platform will also allow the salon to send personalized text-based SMS messages to consumers' mobile phones. By analyzing intervals of client appointments, the salon can remind shoppers of their last service and when they are due for a visit or touch up.

"It can also be a call to action," he explains. "It can alert a client to her favorite stylist's available appointments for the next couple of days in hopes of prompting her to visit."

Retailers can also deliver these timed-based marketing campaigns, as well as surveys and contests, to an individual, selected client group, store or region. "For example, a marketing manager can decide at 9 a.m. to launch a campaign good only for today," TalentBeat's Moran explains. "This can help boost sales and drive additional traffic into the stores."

The final piece of the puzzle is to reward shoppers for "redeeming" these promotions. After accessing redemption information stored in a database available in the cloud, they can gain insight into their best clients and reward them for their loyalty. "Whether they send a coupon or deliver a discount, the targeted incentives are a way to boost loyalty and retain shoppers," adds STOREWORKS' Stelzer.

The chain will be able to do so by leveraging some unique features of VeriFone's MX880 device. Besides a full keypad for PIN debit transactions, a robust GUI interface also enables the merchant to deliver a customer dashboard that allows them to sign up for the loyalty program, check their membership status and redeem incentives.

The retailer plans to leverage its loyalty platform by the first quarter of 2013.