THE APPLICATION OF PCI AND BEYOND - SECURING CONTACT CENTRE PAYMENTS

CHERYL ODEE HELM

Cheryl Odee Helm is a contact centre consultant at Helm Communications, a firm that helps companies to design, select, and implement contact centre technologies. Cheryl is a member of the Community of Telecommunications Consultants (CTC) *and can be reached at (905) 985-4555 or cheryl@helmcomm.com.*

PCI DSS (Payment Card Industry Data Security Standards) applies to all organizations that store, process or transmit cardholder information. Fraud prevention technologies and services are already well developed. Encryption exists to segregate card data between Chip and PIN devices and Point of Sale machines. Payment pages can be hosted by the merchant's Payment Service Provider (PSP). However, none of these approaches can be deployed by the contact centre to protect telephone payments, whose vulnerabilities fall into four distinct areas:

- Physical contact centre environment
- Call and screen recordings
- VoIP and telephony network
- Agent desktops and data network

Bob Russo, the General Manager of the PCI Security Standards Council, is a tireless advocate for multilayer security. He has been widely quoted as saying "compliance does NOT equal security". What Russo means is that employing PCI standards is the start of journey, not the end. Compliance is Step One in protecting your contact centre. Step Two is applying additional security solutions.

Is your contact centre PCI compliant? Whether a company internally files an annual Self-Assessment Questionnaire (SAQ) or works with a Qualified Security Assessor (QSA) and files an annual Record of Compliance (ROC), there could be as many as 288+ controls with which one needs to comply. When I consult with contact centres about PCI compliance, I point them to two key documents that can be downloaded from the PCI website (https://www.pcisecuritystandards.org). The first document describes the actual "288+ controls" (SAQ-D). The second document is a special supplement from PCI, with additional security requirements for contact centres, called "Protecting Telephone-based Payment Card Data".

PCI wants merchants and organizations to protect payment card data in all sales channels; contact centre, website, mobile, card present and card not present transactions. When applying these standards to a contact centre, one must identify all the systems, applications, tools, networks and desktops that touch or interact with card data. Compliance includes how contact centre agents take payments over the telephone. Agents typically ask customers to verbally state their payment or credit card numbers. They will then often repeat back the numbers for clarity and may also write down numbers on their computer notepad or on actual note paper so that they don't make mistakes or it allows them to use the numbers for multiple transactions. I have taken tours of many different contact centre environments and seen this done over and over again. Can I go into your trash bins or agent notebooks and find credit card numbers?

Many organizations are compelled and sometimes required to record conversations with customers regardless of the fact that these conversations may include sensitive information about payment card data. PCI DSS regulations prohibit the recording of card data, leaving an organization with the dilemma of two conflicting requirements: how to record the call without recording the payment card information?

A technique used to remove card data from call recordings is called "pause call resume". It can sometimes be automated, however many vendors offer systems that require the agent to manually pause the call or screen recording during the portion of the call in which the agent and customer are verbally discussing and repeating payment card numbers (call recording) or where the agent is typing numbers into the billing application or payment screens (screen recording). There are vendor solutions available called "redaction tools" that will help to remove payment card data from call recordings.

PCI standards also apply to the use of a payment through an IVR (interactive voice response) system. This is a type of IVR that asks customers to enter payment card into the telephone keypad. Customers typically get transferred to a payment IVR by a self-service menu selection or by a contact centre agent when payment processing is needed during a live call. PCI compliance documents require an organization to state that any use of payment IVRs protects payment card data. When selecting a payment IVR, make sure to choose a solution that "flattens" the keypad (DTMF) tones. This means that the tones all sound the same. Someone with access to the call recording would not be able to determine what the payment card numbers are by listening to the recorded keypad tones.

How much does PCI compliance cost? I have researched this question and found many different answers. The most common answer is "We're not quite sure but we know we have to do it." I recently came across a contact centre security vendor called Semafone that provides a series of "PCI Cost Calculator" spreadsheets. They use these spreadsheets to help cost justify the value of their product. Semafone was able to provide some interesting information.

Small Firms and Mobility

More than 75% of SMBs used mobile technology this year, up from two thirds last year, according to a survey of 540 SMB owners by Constant Contact. About 92% of SMBs either have deployed or are interested in deploying mobile-optimized website. 21% of the respondents said they are using mobile advertising, up from 10% last year. Another 23% said they were interested in using mobile advertising this year.

Do You Want to Manage Mobility?

More than 55% of IT managers are either planning to outsource mobility management or have already done it, according to a recent survey by Gigaom Research. Mobile management includes mobile strategy, planning, provisioning, management and contracts. Mobility represents an increasing expense in most enterprises and mobility management is often considered a non-IT responsibility.

Tablets: Market Caps

Q2 2014 confirmed the trend of the previous quarter: tablet sales leveled off – an increase of only 4.7% compared to 2013. We predicted it in June, after the release of Q1 2014 data. It's easy to increase sales in an untapped market, but when more than 50% already have a great tablet in their hands, they will not change it every year. In fact, the tablet market will soon resemble the computer market: a stable, mature, essentially replacement market.

Videotron: 4th National Wireless Operator?

Pierre Dion, Videotron's new CEO, stated at last June's Canadian Telecom Summit: "Our vision is to provide Canadians with a new high-quality, low-cost wireless choice and real wireless competition. Under the right conditions, we are ready, willing and able to become Canada's fourth wireless competitor." Earlier this year, Videotron bought access to spectrum in British Columbia, Alberta and Ontario.

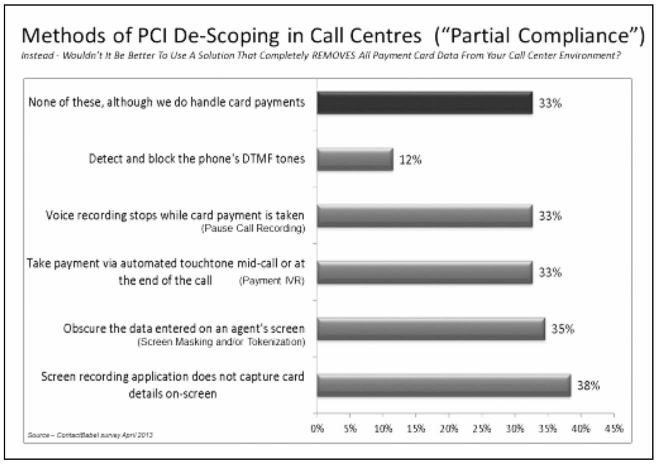
The spreadsheets were built by an independent QSA firm (Foregenix) and looked at the cost of implementing all 288+ PCI controls, plus additional information like network costs, hardware and equipment costs, employee costs, etc. The spreadsheets consistently found that whether the contact centre has 50-100, 1,000, or 10,000 agents, it will cost between $3,000 and $5,000 per agent/desktop per year to setup and maintain PCI. Semafone provided customer references that have extensively examined the spreadsheets and have tried to break or disprove them. However, in the end they also came up with the similar figures of $3,000 to $5,000 per desktop per year.

The shortcomings of PCI. PCI is necessary to provide protection of sensitive information and we all must implement PCI, however, "compliance does not always equal security". For example, after spending $3,000 to $5,000 per agent/desktop per year to implement and maintain PCI in your contact centre environment, your agents can still see and hear payment card data! Your agents can still write down payment card numbers. PCI standards say that you must remove paper, pens, and cellphones from contact centre environments, but few centres have implemented these strict rules, and people are clever – especially if they can still see and hear the information. Organized hacking schemes can take place. This situation exists even in most "PCI Compliant" outsourcing environments.

"We only hire good people". I recently heard the following true story. At a major U.S. contact centre outsourcer, a security guard found a cellphone on the floor in the men's bathroom. The guard picked up the cellphone and turned it on to see who it might belong to. On the screen was a long series of numbers. The guard brought the phone to security. Security determined that in fact, the string of numbers were payment card numbers. A contact centre agent was carefully and secretly copying payment card numbers into his cellphone as he was listening to customers repeat them for him during telephone conversations!

"We do background checks on all our people". There was another example of a contact centre agent who was part of an organized hacking team. He wore a secret extra earpiece under his employer-provided headset that transmitted the agent/customer conversation to an outside source which recorded customer names, addresses, and payment card data. The agent carried a USB device which he plugged/unplugged into his PC daily which also recorded customer data. When he was caught, he confessed that he was part of an organized group who had obtained thousands of payment card numbers with corresponding names and addresses. They had purchased their USB recording devices and earpiece transmitters on the internet for less than $100.

The following 2013 survey illustrates that approximately 33% of the contact centres do not comply with PCI standards. Furthermore, of those that do, it reveals the methods used by organizations in handling the sensitive credit card information in contact centres:


Methods of PCI De-Scoping in Call Centres ("Partial Compliance")

Instead - Wouldn't It Be Better To Use A Solution That Completely REMOVES All Payment Card Data From Your Call Center Environment?

Source – ContactBabel survey April 2013

Beyond PCI. There is another method to consider – why not completely remove card data from contact centre environments? There is a new series of security tools emerging in the market. Semafone, mentioned previously, is a good example. It provides security applications that get installed in your contact centre environment, connect into the telephony lines, integrate into the payment card fields, and connect directly to your payment gateways. Semafone collects payment card numbers from your customers through the telephone keypad (like a payment IVR), which prevents the agent/CSR from hearing or seeing any card data, then it sends the card data directly to your payment processor.

Protecting your customers. Essentially, these new contact centre security tools clearly offer two advantages. They completely de-scope your contact centre from PCI. They can remove all payment card data from touching or storing payment card numbers within all systems, applications, tools, networks, and desktops. They work like a payment IVR and prevent your contact centre agents from seeing and hearing any payment card data. When using these new security tools, there is no need to use "pause call resume" with call/screen recording because payment card data has been reduced to a series of flattened phone keypad tones (instead of audible voice). Furthermore, another key benefit is that the agent can stay on the call during the entire process to offer assistance and customer support. These new security tools can save organizations money; they cost far less per desktop per year ($3,000 - $5,000) than implementing and maintaining the PCI standards, yet go beyond PCI.

In conclusion, PCI DSS is vital and necessary to protect client payment card information. The PCI standards must be implemented within contact centres. However, it is a good idea to check out vendors that offer new security tools available that can save time, money, and effort and surpass the PCI requirements.