Five Tips for Achieving PCI Compliance in Your Contact Center

Keeping customer payment card data protected is a concern for many organizations, but it's especially important in contact centers, which are intrinsically vulnerable to data security threats.

Since contact centers are awash in customer information (such as credit card numbers and personal identification data) and tend to have relatively high staff turnover, they can be fertile ground for exploitation by data thieves. Moreover, as centers hire an increasing number of remote employees, the potential for data compromise can increase further still.

The Payment Card Industry Data Security Standard (PCI DSS) was created in 2004 to protect payment card information. Since then, the standard has evolved to address new threats. If your contact center is planning its strategy for PCI DSS compliance, here are some tips to help you get started:

1. Leverage the resources on the PCI Standards website.

The standard itself, along with FAQs, supplemental guides, and a **PCI Quick Reference Guide**, are provided by the PCI Security Standards Council (PCI SSC) website located at **www.pcisecuritystandards.org**. The Quick Reference Guide offers an overview of the standard and security controls required for compliance. Consider reading this document first, and then moving on to the standard and other supporting documents.

It's good practice to visit the PCI DSS website periodically to stay abreast of changes, since they could impact your contact center significantly. For example, in March 2011, the PCI SSC released a supplement providing specific guidance for protecting telephone-based payment card data. Most contact centers record calls and review them for quality purposes, which can be an effective way to spot fraudulent behavior and help ensure compliance with a variety of regulations. However, recorded calls that contain specific card information can themselves be used to perpetrate fraud. The supplement tackles this issue and provides a decision process for protecting voice recordings in accordance with PCI DSS 2.0. In May 2015, PCI DSS 3.1 issued guidance to migrate from Secure Sockets Layer (SSL) and Early Transport Layer Security (TLS) to TLS v1.1 or higher.

2. Engage with your contact center technology vendors.

The PCI SSC supports the use of technologies involved in processing credit card transactions. Its goal is to ensure that *payment system information* is compliant. Seek guidance from your technology vendors and ask how their solutions can help you achieve PCI compliance. The PCI SSC website provides a list of payment applications that meet the Payment Application Security Data Standard (PA-DSS). Selecting a tool from this list can help ensure compliance in that area.

But what about other technologies and systems that are used in conjunction with payment processing, although not part of the payment processing application per se? For call recording and other technologies that are within scope for PCI DSS but not involved in the processing and settlement of payments (and as such, are ineligible for PA-DSS), those vendors should still have the resources to help you achieve PCI compliance leveraging their technology. Look for recording solutions with AES 256-bit, end-to-end encryption, and the ability to automatically trigger the recorder to pause and resume based on employee desktop activity. This helps avoid capturing sensitive authentication data, such as CVV2 codes.

3. Keep personal data confidential.

Don't just stop at protecting payment card information when increasing security across your data center. Remember that confidential data elements are identified in the state breach notification laws, and credit card data is just one item on that list.

When you look at cost-justifying mechanisms and what needs to be protected, consider all types of personal data, such as social security numbers, driver's license numbers, birth dates, mother's maiden names, medical records, and more.

4. Don't overlook physical layout issues.

Traditional contact center layouts that promote easy monitoring and access to supervisors can sometimes present unique security challenges. Do you have an open floor plan? If so, consider creating a "clearance" area for the contact center employees authorized to take credit card numbers. This helps protect other employees from overhearing conversations or "shoulder surfing" — viewing sensitive on-screen information.

5. Consider work-at-home employees.

Remote workers, including contact center employees, may have special requirements pertaining to PCI DSS. If you have work-at-home employees who have exposure to payment card information, careful security screening and processes are in order. Two-factor authentication (such as hardware tokens) can help ensure the approved employee is the person logging in and accessing secure information. Some companies are even instituting voice biometrics technology to help ensure the person on the phone is the authorized employee. Strict security policies, training, and frequent audits are important. Using a firewall to keep remote employees on a separate segment of the company network can be an additional way to limit security and data breaches. Focused, analytics-driven quality management can also help ensure staff follow PCI compliance processes.

Although PCI DSS can present a challenge for organizations that need to comply, many data security experts consider these steps as the minimum for protecting consumer information. Your customers expect and deserve this protection — and your company's reputation may depend on it.

Americas
info@verint.com
1-800-4VERINT

Europe, Middle East & Africa
info.emea@verint.com
+44(0) 1932 839500

Asia Pacific
info.apac@verint.com
+(852) 2797 5678

verint.com
twitter.com/verint
facebook.com/verint
blog.verint.com