SANS SECURITY AWARENESS

Managing Human Risk for PCI DSS Compliance

Frequently Asked Questions and Tip Sheet

Credit cards have become the primary way people make purchases, especially with the growth of online shopping. Credit cards are incredibly convenient, allowing people to make large purchases almost anywhere in the world. However, credit cards also have risks. Cyber criminals are actively trying to steal credit card information. Once in possession of this information, they can create physical copies of the credit card or simply use the information for online purchases. The more credit cards criminals steal, the more money they can make. As a result, many criminals no longer target individuals, and have moved towards commercial organizations that store, process, or transfer cardholder data.

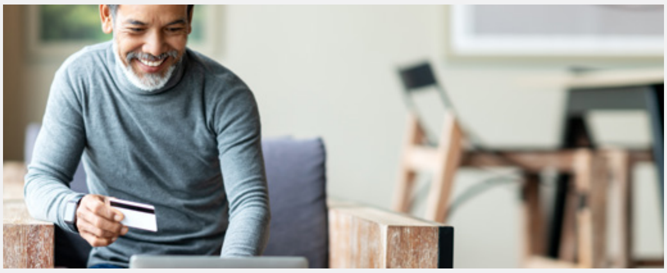
PCI DSS was created to help organizations better safeguard the cardholder data they handle on a daily basis. The following pages will help you better understand PCI DSS and provide you with some tips for upholding your organization's responsibilities with respect to the standard as they relate to human risk.

What is PCI DSS?

The Payment Card Industry Data Security Standard (commonly called PCI DSS) provides clear and common requirements for protecting cardholder data. These requirements are important for any organization that stores, processes, and/or transmits cardholder data.

Why was the standard created?

To reduce credit card fraud, five members of the payment card industry (Visa, MasterCard, American Express, Discover, and JCB) joined together to develop specific security standards for any organization that stores, transmits, or processes cardholder data. Any organization that handles cardholder data must understand and abide by these rules.



Is my organization required to be PCI DSS compliant?

In all likelihood, yes! PCI DSS compliance is required for any organization that accepts credit card payments. The level of compliance required and the complexity of any compliance audit will depend on the volume of credit card transactions your organization processes.

Doesn't my IT department have these compliance requirements covered?

Not entirely! While some of the requirements for PCI DSS compliance are technical in nature, such as the requirement to install and maintain a firewall to protect cardholder data, much like any other security initiative, PCI DSS compliance begins and ends with the human factor. For example, the establishment of and training on standardized procedures for the processing of payment card information is essential to demonstrating compliance.

Examples of Cardholder Data

There are a variety of different types of information that can make up cardholder data. It is any information that is the combination of the credit card number (Primary Account Number, or PAN) and any other related information. Other types of data that would be considered cardholder data when combined with this would include:

- The cardholder's name, billing address, or telephone number.
- The card's expiration date.
- The card's security code. This is a three-digit value usually written on the back.
- The card's PIN. This number should not be confused with the PAN. A PIN is the cardholder's password entered at the time of transaction and should never be recorded, printed, or stored.

What are some ways I can mitigate the human factor to achieve and maintain PCI DSS compliance?

As with any security and compliance initiative, proper training is essential for success. Depending on the size of your organization, the different job functions involved in processing and storing payment card information, and the number of transactions your organization processes, that training may take on different forms.

Below are some quick tips to get you started on your journey towards PCI DSS compliance.

1. Multi-factor authentication is required for any person accessing computers where card data is handled. Multi-factor authentication means that at least two methods are used to verify a person is who they say they are.

2. You must limit access to cardholder information and payment systems to only those users whose jobs require access and who have authorization to access them.

3. Primary Account Numbers should be rendered unreadable, typically through encryption, whenever they are stored using organization-approved methods. In addition, employees must never send unencrypted account numbers through email, instant messaging, or social media sites.

4. Any system that stores, processes, or transmits cardholder information should only be used for that purpose. It should never be used for non-work related or unauthorized activities, such as accessing personal email accounts or browsing the Internet.

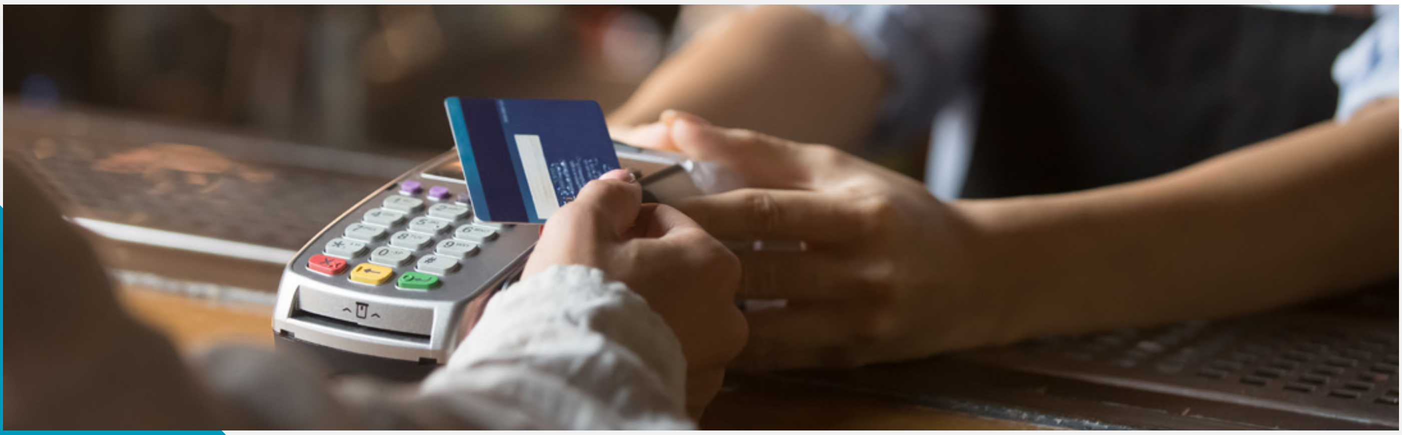
5. Under no circumstances may you store any sensitive authentication data, such as the user's Personal Identification Number (PIN), three or four-digit verification code, or full details of the payment card's magnetic track data.

6. If your organization operates point-of-sale registers to process customer payments, you need to follow additional requirements that include:

   - Verify the identity of any third party claiming to be a maintenance or repair person for payment card devices before granting them access to the device. Criminals often pose as repairmen when attempting to compromise a payment card device.

   - Before installing, replacing, or returning a payment card device (or allowing a third party to do so), make sure you have received verification from your supervisor.

   - Maintain awareness of any suspicious behavior occurring around a payment card device, like people trying to unplug or open the device. If you observe this, report it immediately to your supervisor.



Ensuring your workforce respects these guidelines, will help uphold your obligation to protect your customers' cardholder information and maintain compliance with industry standards. For more information, or to learn more about how role-based PCI DSS training can simplify compliance, contact us here.

Ready for more? Try our role-based PCI DSS course.

Traditionally, PCI DSS compliance has been challenging to implement enterprise-wide because the responsibilities for compliance differ greatly from one role to another. Our role-based training allows you to customize training tracks by assigning relevant topics based on each employee's unique role. This approach simplifies the delivery of targeted training, enhancing engagement, retention, and overall effectiveness.

Visit https://go.sans.org/lp-demo-request-pci-training to learn more.

About SANS Institute

Established nearly 30 years ago, SANS Institute was created as cooperative research and education organization that offers programs to over 165,000 security professionals. SANS is the most trusted and largest source for information security training and security certification in the world—leverage our best-in-class Security Awareness solutions to transform your organization's ability to measure and manage human risk.

SANS SECURITY AWARENESS