**Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 95 – 99 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# CHALLENGES OF IMPLEMENTING THE PAYMENT CARD DATA SECURITY STANDARD (PCI DSS) IN PRACTICE

Audrius Lopata, Kaunas University of Technology
audrius.lopata@ktu.lt

**ABSTRACT:** The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem. Challenges of Implementing the Payment Card Data Security Standard (PCI DSS) in Practice presented in this article

**KEYWORDS***: PCI DSS, Cyber security, Payment Gateways, Security standards*

## BRIEF SUMMARY ABOUT PCI DSS STANDARD

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework designed to secure payment card data handling. It was established by the Payment Card Industry Security Standards Council (PCI SSC), comprising major credit card companies like Visa, MasterCard, American Express, Discover, and JCB. The standard applies to all entities involved in card payment processing, including merchants, processors, and service providers.

Key goals of PCI DSS include:

1. Protect Cardholder Data: Safeguarding sensitive data, such as card numbers and security codes, through encryption and secure storage.
2. Implement Strong Access Controls: Restricting access to cardholder data to authorized personnel only.
3. Maintain a Secure Network: Ensuring robust firewall configurations and secure network protocols.
4. Regular Monitoring and Testing: Conducting routine audits, vulnerability scans, and penetration testing to identify and mitigate risks.
5. Develop a Security Policy: Promoting a security-conscious culture through documented policies and employee training.

The standard is divided into 12 key requirements covering areas like network security, vulnerability management, and monitoring. Compliance is mandatory for businesses handling payment cards and is enforced through audits and penalties. By adhering to PCI DSS, organizations can mitigate risks of fraud, data breaches, and financial loss while ensuring customer trust.

## PCI DSS COMPLIANCE LEVELS

These levels categorize businesses based on the volume of annual payment card transactions. Below is a brief summary of these compliance levels:

Level 1: For businesses processing over 6 million transactions annually or those that have experienced data breaches. This level has the most rigorous requirements, including an annual audit by a Qualified Security Assessor (QSA) and quarterly network scans.

Level 2: For businesses processing 1 to 6 million transactions annually. They typically need to complete a self-assessment questionnaire (SAQ) and conduct quarterly network scans.

Level 3: For businesses processing 20,000 to 1 million e-commerce transactions annually. They also complete a self-assessment questionnaire and perform quarterly scans.

Level 4: For businesses processing fewer than 20,000 e-commerce transactions annually or up to 1 million other payment card transactions annually. This level has the least stringent requirements but still includes completing an SAQ and conducting quarterly scans.

## PCI DSS – 5 MOST COMMONLY OBSERVED CONTROL FAILURES

**Challenge No.1**

It is of utmost importance for businesses dealing with cardholders' data to be aware of the locations where the data resides. However, most businesses have failed to do so only because a lot of payments card data remains unmanaged and uncategorized, dispersed across multiple databases of an enterprise.

Proposed Solution:

To meet this PCI DSS compliance control, businesses must map the business systems through which the cardholder data enters the organization and leaves all the way through.

To establish a diagram that shows how cardholder data flows across systems and networks, businesses can depict the cardholder data environment, devices and systems with all payment channels, applications and associated protections on CHD based on locations, using a labelling method for identifying the transport mechanism and crucial dependencies.

**Challenge No.2**

Many businesses even though have established security policies, they fail to maintain the same that open multiple vulnerabilities in the payments lifecycles.

This has been noticed to happen with companies that have documented and published a security policy for the PCI DSS compliance requirement but have not actually used them.

Proposed Solution:

When creating a security policy for the PCI DSS compliance requirements, the organizational design must be brought into work. First and foremost, create a policy to address every requirement of PCI DSS and ensure that it is structured to match the order and language of the PCI DSS sub requirements.

Moreover, businesses must review and update at least annually to effectively maintain the security policy.

**Challenge No.3**

Tracking card data is directly proportional to tracking the people that process and store it.

However, most of the businesses attempting to comply to PCI DSS compliance requirements fail due to this important control. It happens only because companies do not track the devices well.

Proposed Solution:

Assurance and operations members of risk and compliance teams must update the device lists with changing employees. The best solution to tackle this PCI DSS control is to maintain an accurate inventory with proper labelling and set a shorter frequency for updating the list with 4 columns – device, employee, data type, and access type.

**Challenge No.4**

Off-the-shelf security incident response plans remain outdated and ineffective against the ever-changing threat landscape. For compliance analysts and managers, verification of plans only goes so far.

Each year, SISA performs hundreds of incident response exercises across the globe.

During these engagements, we have observed incident response plan failures mostly because of organizational shortcomings that form a major part of the PCI DSS requirements. Failing to plan means planning to fail.

Proposed Solution:

Businesses opting to verify their incident response plans for PCI DSS compliance must simulate a real-world attack every 6 months and assess how key stakeholders respond to it.

Operational security teams must, in such events, document issues and lessons against specific scenarios of PCI DSS incident response requirements including organizational coordination, business recovery, data backup, and analysis of legal requirements.

**Challenge No.5**

All data custodians and key management professionals that give access to data based on a business' need to know must be solely responsible to monitor the access hygiene.. However, businesses ignore

the importance of bestowing this responsibility to an individual with formal accountabilities This has become crucial ever since remote working has increased as companies aren't able to ensure that the type of access given is appropriate and all technical safeguards are in place for data access.
Proposed Solution:
A data security specialist with a straight-line reporting to the executive authority of the firm (CIOs, CISOs, Information Security Managers, Chief Data Officers, Risk and Compliance Managers, etc.) must be nominated for such responsibilities. QSAs at SISA recommend such professionals to implement privileged access management and update the data access charts on a monthly basis.

## MAIN RECOMMENDATIONS HOW TO SUCCESSFULLY IMPLEMENT THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

### Understand PCI DSS Requirements

Familiarize with PCI DSS version: Ensure that you are working with the most current version of PCI DSS (as of 2024, it's v4.0).
Identify scope: Understand which systems, processes, and personnel are involved in the storage, processing, or transmission of cardholder data.
Review the 12 PCI DSS requirements: These include securing network systems, protecting cardholder data, maintaining a vulnerability management program, and monitoring network access.

### Scope and Segmentation

Define scope: Identify all locations where cardholder data is stored, processed, or transmitted. This includes all systems that can affect the security of the cardholder data environment (CDE).
Network segmentation: Implement network segmentation to isolate systems that handle cardholder data from other parts of your network, reducing the compliance scope.

### Create a PCI DSS Compliance Team

Appoint a compliance manager/team: A dedicated team should oversee the implementation of PCI DSS standards.
Cross-functional collaboration: Include members from IT, security, legal, and operations to ensure all areas are covered.

### Data Protection Measures

Encryption: Ensure sensitive cardholder data is encrypted both in transit (e.g., SSL/TLS for web traffic) and at rest (e.g., disk encryption).
Masking and truncation: Mask PAN (Primary Account Number) where necessary and store only the minimal necessary information.
Secure storage: Avoid storing sensitive authentication data (e.g., CVV, magnetic stripe) after authorization unless absolutely necessary.

### Access Control

Limit access to cardholder data: implement strong access control measures, ensuring only authorized personnel can access the cardholder data environment (CDE).
Role-based access: Enforce role-based access control (RBAC) with the principle of least privilege.
Two- factor authentication: Use multi-factor authentication (MFA) for personnel accessing critical systems.

### Regular security testing

Vulnerability scanning: Conduct regular internal and external vulnerability scans.
Penetration testing: Perform annual penetration testing to identify vulnerabilities in the systems.
Application security testing: Ensure secure software development practices by conducting code reviews and application vulnerability testing.

**Monitoring and logging:**
Log management: Implement logging mechanisms to track access to network resources and cardholder data.
Intrusion detection and monitoring: Utilize tools to monitor network traffic and alert administrators of suspicious activities.
Retain logs: Store logs for at least one year, with the last three months available for immediate review.

**Regular Audits and Assessments**
Self-assessment questionnaire (SAQ): Smaller merchants may be required to complete an SAQ annually.
Qualified Security Assessor (QSA) audit: For larger organizations, hire an external QSA to perform annual assessments and provide formal validation.
Gap analysis: Conduct a gap analysis to identify areas that need improvement before formal audits.

**Emploee training and awareness**
Security awareness training: Provide regular training on PCI DSS requirements, phishing, and secure handling of cardholder data.
Incident response training: Ensure that personnel are familiar with the organisation's incident response procedures in case of a security breach.

**Incident Response Plan**
Develop a plan: Establish an incident response plan for handling security breaches that involve cardholder data.
Test regularly: Regularly test and update the incident response plan to ensure effectiveness.
Notify stakeholders: Have a communication plan to notify necessary stakeholders, including banks, card brands, and customers, in the event of a breach.

## CONCLUSIONS

The implementation of the Payment Card Industry Data Security Standard (PCI DSS) is essential for businesses handling payment card data to ensure its security and maintain customer trust. While the framework provides robust guidelines for safeguarding cardholder data, its practical application poses significant challenges, such as identifying data locations, maintaining effective security policies, tracking data and devices, updating incident response plans, and ensuring proper access controls. Addressing these challenges requires comprehensive strategies, such as mapping data flows, creating and maintaining security policies, appointing dedicated compliance teams, and leveraging advanced tools for encryption, logging, and monitoring.
Successful PCI DSS implementation involves a clear understanding of requirements, proper scoping and segmentation, regular testing and audits, and fostering a culture of security awareness. Organizations must also invest in employee training, simulate real-world scenarios for incident response, and establish effective collaboration across departments. With these measures, businesses can overcome the hurdles of PCI DSS compliance, enhance their security posture, and reduce the risk of fraud or data breaches, thereby safeguarding both the business and its customers.

## ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES:

1. Stephen Hancock, PCI DSS Version 4.0 - A guide to the payment card industry data security standard. Released February 2024. Publisher(s): IT Governance Publishing, ISBN: 9781787785090

2. Arthur B. Cooper Jr. (Author), Jeff Hall (Author), David Mundhenk (Author), Ben Rothke (Author). The Definitive Guide to PCI DSS Version 4: Documentation, Compliance, and Management 1st ed. Edition
3. Chad M. Barr (Author). Fortifying The Digital Castle: A Strategic Guide to PCI DSS Compliance and Cyber Defense Kindle Edition 2024
4. Branden Williams (Author), James Adamson (Author)PCI Compliance 5th Branden Williams (Author), James Adamson (Author) Publisher: CRC Press; 5th edition (December 22, 2022). ISBN-13:978-0367570033
5. PCI DSS: A pocket guide (Compliance) 6th Edition by IT Governance (Editor) 2019, ISBN-13 : 978-1787781627
6. Bharat Nishad, PCI DSS Compliance Masterclass - Foundation to Mastery, ASIN : B0CWPPGPQS, Publisher : Bharat Nishad (February 26, 2024).
7. PCI Compliance A Complete Guide - 2021 Edition Paperback – December 17, 2020 by The Art of Service - PCI Compliance Publishing (Author), ISBN-13: 978-1867414933
8. ENYINAYA OKAFOR, The Plague Of Cyber Threats In The Financial Industry: PCI-DSS COMPLIANCE Kindle Edition, February 29, 2024, ASIN : B0CW1HM6JR