Joshua Farias

Professor Cooper

SEC 605

11th February 2024

Project Part 1: PCI DSS Compliance

Introduction

In the digital age, ensuring the security of credit card transactions is critical for any businesses operating online. For S&H Aquariums, the protection of our customers' credit card information is not only a matter of trust but also a necessity. This report outlines the Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, and the considerations S&H Aquariums must address to secure cardholder data effectively.

PCI DSS Overview

The PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. The standards are founded on six control objectives with twelve high-level requirements to meet the PCI DSS standard:

1) **Build and maintain a secure network:**
    - **I.** Install and maintain a firewall configuration to protect cardholder data.
    - **II.** Do not use vendor supplied defaults for system passwords and other security parameters.

2) **Protect cardholder data:** Cardholder data must be safely stored and protected utilizing secure encryption standards during transit and at rest.
    - **III.** Protect stored cardholder data.
    - **IV.** Encrypt transmission of cardholder data across open, public networks.
3) **Maintain a vulnerability management program:** Systems must be secured, keep software up-to-date and are required to utilize antivirus software.
    - **V.** Use and regularly update antivirus software or programs.
    - **VI.** Develop and maintain secure systems and applications.
4) **Implement strong access control measures:** Restrict access to cardholder data on a need-to-know basis requiring physical controls and unique IDs for everyone accessing the cardholder's data.
    - **VII.** Restrict access to cardholder data on a need-to-know basis.
    - **VIII.** Assign a unique ID to each person with computer access.
    - **IX.** Restrict physical access to cardholder data.
5) **Regularly monitor and test networks:** Access to cardholder data must be monitored and periodic penetration testing of the network must be conducted to identify any potential security vulnerabilities.
    - **X.** Track and monitor all access to network resources and cardholder data.
    - **XI.** Regularly test security systems and processes.
6) **Maintain an information security policy:** Security policies must reflect the requirements outlined by the PCI DSS and an awareness program must be implemented to educate employees on potential security risks.
    - **XII.** Maintain a policy that addresses information security for employees and contractors.

Why PCI DSS Compliance is Need and Consequences of Failing to Comply

Compliance with PCI DSS is an essential requirement for any business that handles credit card transactions. Compliance demonstrates to customers and business partners that S&H Aquariums is committed to securing their data. Failure to comply with the PCI DSS can result in significant fines, increased transaction fees and even the termination of the company's ability to accept credit card-based payments. More importantly, a breach could significantly destroy the trust and reputation of S&H Aquariums with its customers and business partners.

Immediate Considerations for PCI DSS Compliance

Given the projected transaction total being between 20,000 and 1,000,000 in the first year, S&H Aquariums will likely qualify as a Merchant Level 3, requiring a specific level of compliance verification requirements such as the Self-Assessment Questionnaire (SAQ), a quarterly external vulnerability scan by an Approved Scanning Vendor (ASV), and the completion of an Attestation of Compliance Form.

- **Payment Brands**: Initially accepting MasterCard and Visa simplifies compliance because these companies do not have additional sets of compliance requirements such as American Express and Discover. Instead, Visa and MasterCard have programs that outline how merchants should implement PCI DSS requirements and validate compliance in the forms of the Cardholder Information and Security Program (CISP) for Visa and the MasterCard Site Data Protection (SDP) for MasterCard.

Future Considerations for PCI DSS Compliance

- **Volume Increases**: Surpassing 2.5 million American Express or 6 million Visa, Mastercard or Discover transactions will elevate S&H Aquariums to Merchant Level 1, requiring an Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA) in addition to the prior requirements outlined as a Level 3 Merchant.
- **Accepting Additional Payment Brands**: The integration of brands such as American Express or Discover will necessitate adherence to their specific guidelines in addition to PCI DSS standards such as the Data Security Operating Policy (DSOP) for American Express and the Discover Information Security and Compliance (DISC) for Discover.
- **Brick-and-Mortar Storefronts**: Opening physical stores introduces the need for securing point-of-sale (POS) systems and networks within these storefronts, further emphasizing the importance of PCI DSS compliance across different transaction environments.

Conclusions

Ensuring PCI DSS compliance is a process that requires careful planning and consistent effort. For S&H Aquariums, it is essential for building a secure and trustworthy platform for our customers. As we grow and expand our payment options and sales channels, our commitment to security and compliance must evolve accordingly. This report serves as a foundation for our compliance, emphasizing the need for strategic planning, education, and investment in security measures.

Resources:

Johnson, R., Weiss, M., & Solomon, M. G. (2022). *Auditing IT Infrastructures for Compliance*. Jones & Bartlett Learning. (p. 37).

PCI Security Standards Council. (n.d.). *PCI DSS Quick Reference Guide*. Retrieved from https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Reciprocity. (n.d.). *What is PCI Compliance Level 1?* Retrieved from https://reciprocity.com/resources/what-is-pci-compliance-level-1/

PCI Policy Portal. (n.d.). *Merchants*. Retrieved from https://pcipolicyportal.com/what-is-pci/merchants/

Visa. (n.d.). *PCI DSS Compliance Information*. Retrieved from https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html

MasterCard. (n.d.). *Site Data Protection - PCI*. Retrieved from https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html