PCI DSS COMPLIANCE

Ryan Rockett, Marcos Vallejos, Luis Ruiz, Madina Yusufzai
TEAM FOUR

Contents

Introduction

When a customer purchases items at a store, the transaction goes so fast that it almost seems like magic. Swipe the card and voila, the items are purchased. In reality, there are a lot of moving parts that go into each transaction. To function smoothly, there needs to be a standardized way in which payments are processed and how that information is protected. This need gave rise to the Payment Card Industry Data Security Standard, more commonly known as PCI DSS. Using this standard, organizations are given steps to process card payments, store cardholder data, and transmit credit and debit card information across open public networks. Understanding why the PCI DSS is important and identifying the organization's current and future considerations will allow S&H Aquariums to be better placed to proceed to grow while remaining compliant.

PCI DSS Overview

The Payment Card Industry Data Security Standard, more commonly known as PCI DSS, is an industry self-created standard that is used to standardize the receipt of credit card payments. Depending on the level of volume of credit card processing that a company performs, there are different thresholds that once achieved may cause the company to become compliant with higher levels of standards outlined in the Payment Card Industry Data Security Standard. There are three main ongoing practices that a company must undertake, six main principles that a company must adhere to, twelve primary requirements for those companies, and several sub requirements that are dependent upon the industry that the company is a part of. Using these tools to maintain compliance, companies are better equipped to maintain the security of their clients' data.

The three main ongoing requirements that come from the PCI DSS are Assessing, Remediation, and Reporting. To meet the requirement for assessing, a company must be able to identify the cardholder data in addition to being able to identify all of the related information technology infrastructure and processes within. To achieve this goal, a company must make sure that adequate controls are in place and test those controls for vulnerabilities on a regular basis. Once this has been achieved, a company may then move to remediation. In order to remediate, a company would need to eliminate the storage of unnecessary data and patch any uncovered vulnerabilities from the assessing step. The last of the ongoing requirements is to report. In order for a company to be able to report, it must validate its findings and records of remediation, in addition to then submitting all of the required reports. Only once all three of these requirements are completed is a company adhering to the ongoing requirements of the PCI DSS.

There are six main principles and twelve primary requirements for the PCI DSS, and these two groups go hand in hand together. Within each of the main principles there is a set of requirements that is used to be able to achieve the principle. For instance, the main principle of “build and maintain a secure network” requires that data centers install and maintain a firewall configuration to protect their cardholders' data, as well as not using the default system configuration, passwords, and security parameters that were initially installed from the vendor. Another main principle, protect cardholder data, involves the protection of stored cardholder data and the transmission of that data.

The requirements for this principle are that an organization must secure cardholder data that they are holding, and they must encrypt the transmission of cardholder data across open and public networks. The next main principle involves anti-virus software and the protection of system applications. This principle is to maintain a vulnerability management program. The requirements for this main principle are to use and regularly update anti-virus software and to develop and maintain secure systems and applications. Another main principle involves the curtailing of access to cardholder information, creating unique IDs, and requiring a higher level of authentication. This principle is to implement strong access control measures. The requirements that need to be met in order to achieve this principle are to restrict access to cardholder data to a need-to-know basis, to assign unique identifiers to each person with computer access, and to restrict the physical access to the cardholders' data. The next principle involves the logging and monitoring of the network and regularly testing a company's security system. The requirements to achieve this principle are that an organization must track and monitor all traffic that enters and exits their network, the network resources, and the cardholders' data. The last principle that makes up the PCI DSS involves an organization's security policy. The requirement to achieve this principle is that an organization must maintain a policy that addresses information security for all of its employees and contractors. Using these six main principles and twelve requirements an organization is able to maintain compliance with the Payment Card Industry Data Security Standard.

Rationale

Based on the PCI DSS overview, it is key to understand why these factors are important to S&H Aquariums. There are several reasons that explain why PCI DSS is important to S&H Aquariums. One reason is the confidence of the customers who shop with S&H Aquariums. With this in mind, S&H Aquariums has to be ready for the instance of a data breach. In this instance, if S&H Aquariums is not following the requirements of the PCI DSS, customers would lose faith in the company's ability to keep their information safe, and in turn would stop shopping with S&H Aquariums. This could cause irreversible damage to the reputation of S&H Aquariums, which in turn could slow or even halt the growth of the organization's client base.

Another consideration S&H Aquariums has to think about in regard to PCI DSS is the legal ramifications that could arise from not being compliant with the standard. There are several penalties that could be levied against S&H Aquariums such as monthly penalties and legal action that can result in a loss of revenue. However, if S&H Aquariums is found to have been in compliance, while the organization would still be responsible for the loss of data, the credit card companies may lower the fines or even eliminate them altogether. Lawsuits against S&H Aquariums are also likely to be brought forth in the case of the data breach by the clients whose data was captured. The fines that could be levied against S&H Aquariums for being non-compliant could range from $5,000 a month to a maximum of $100,000 a month. While the penalties ultimately depend on the volume of transactions that S&H Aquariums undertakes, a prolonged series of fines could cripple the organization.

There are a series of best practices that fall in line with the requirements of the PCI DSS, and these can be used to help protect an organization against the loss of cardholder data. One of these best practices would be to buy and only use approved PIN entry devices at the point-of-sale. Some others are to not store any sensitive cardholder data in computers or on paper found at a point-of-sale, to use firewalls on S&H Aquariums networks and personal computers, and to make sure that the wireless router is password protected. While these deal with the data itself, some other best practices are to implement strong password requirements; make sure that all systems are not using the default passwords or security settings; regularly check PIN entry devices and personal computers to make sure that no one has installed rogue software or “skimming” devices such as a keylogger; and lastly, but maybe the most important thing that S&H Aquariums could do, would be to teach employees about security policies, security threats, and the importance of protecting cardholder data.

Immediate Considerations for PCI DSS Compliance

Understanding the requirements for the Payment Card Industry Data Security Standard and the rationale behind why it is important to S&H Aquariums is merely the first step in the process of understanding the organization in relation to PCI DSS. The next major step is to have a full understanding of the way that S&H Aquariums fits into the PCI DSS. There are four main factors that need to be accounted for when establishing how S&H Aquariums fits into PCI DSS, and those are the organization’s accepted payment brands, the volume of transactions, the merchant level of the organization, and the types of reporting that the organization is supposed to maintain and submit.

The first of these four main factors is to determine what payment brands are currently being accepted by S&H Aquariums. S&H Aquariums currently accepts two types of payment brands, Visa and MasterCard. These are the two largest payment brands used in the market today, however, S&H Aquariums does plan to expand its payment options in the future. The organization will begin by adding Discover to the list of accepted payments, and then will later move to accepting those three payment brands and American Express. Having a higher number of accepted payment brands not only increases the transaction volume but will also increase the goodwill with customers because a larger variety of options increases customer satisfaction.

The next main factor is to find the volume of transactions that S&H Aquariums processes in a single year's time. This is important to find as it factors into what merchant level that S&H Aquariums would fall under. Not only is it key to find the total transactions' volume, but it is also important to have a breakdown of each of the payment brands and their transaction volumes. This is used to determine an organization's merchant level. S&H Aquariums processes at least 120,000 transactions each year, with 20,000 of those being from the Visa payment brand and the other 100,000 are from the MasterCard payment brand.

Another main factor is the organization's merchant level. There are four different merchant levels, and each level has specific criteria that has to be met in order for an organization to fall under that merchant level. This is perhaps one of the most important things that an organization has to learn and understand as this is what informs an organization of the types of reporting that must be done. S&H Aquariums processes between 20,000 and 1,000,000 Visa e-commerce transactions per year. It also processes at least 20,000 MasterCard transactions, but does not exceed 1,000,000 transactions with that payment brand. Since these are the only two payment brands that are accepted, and due to the volume of transactions that are processed with these payment brands, S&H Aquarium would be a level 4 merchant.

The last factor is the types of reporting that are needed to maintain the compliance of S&H Aquariums. Because S&H Aquariums is a level 4 merchant, the banking institution that the organization uses may require reports in order to maintain the account. Additionally, there are two other types of reports that are required, those being network scans by an approved scan vendor and a Self-Assessment Questionnaire. The network scan by an approved scan vendor must be completed quarterly and the self-assessment must be completed annually.

Future Considerations for PCI DSS Compliance

For the first year of operations S&H Aquariums will expect between 20,000 and 1,000,000 credit card transactions, and it will not likely exceed 1,000,000 annual transactions in the first couple of years. However, as the business expands it may see over 1,000,000 credit card transactions; this would result in the merchant level of 4 being increased to merchant level 3. The requirements for both levels are the same. To comply with PCI DSS, the company must complete a Self-Assessment Questionnaire and submit an Attestation of Compliance Form. The only difference that will occur would be that the fees for merchant level 4 are higher than merchant level 3. Most potential issues with PCI DSS compliance that S&H Aquariums will face as they expand are not directly caused by the requirements but are caused by the growth itself. With expansion there will be a higher demand on the current IT infrastructure that would not be adequate for the daily traffic that S&H Aquarium’s website will experience. Hackers will also begin to target the company with greater frequency, which could end in data breaches and customer’s personally identifiable information loss. The legal ramifications of a data breach could be costly with legal suits as well as fines from PCI DSS. Ideally, the company does not want to store any customer’s personally identifiable information (PII) so it can circumvent PCI DSS requirements, but it must also take into consideration the ease of transactions as more customers access the site and place their purchases.

In a hosted payment page, S&H Aquariums would not store any customer PII on its website site, but to process the payment, customers would have to temporarily leave the site. This would be a much cheaper alternative than storing customer data and following PCI DSS requirements, and those requirements would fall on the service provider, however, it could also confuse customers as they must leave the site to process their payments. Another viable method is to use an online shopping cart with a customer vault. An online shopping cart will not store any customer PII on S&H Aquarium’s website, however, since no information is stored, the customer must repeatedly input all of their information each time. The customer vault will store that information on a service provider site so that repeat customers have their information retrieved through the service provider’s customer vault. This alternative is more expensive than using a hosted payment page but is still a cheaper alternative than storing information on the company website and having to comply with PCI DSS requirements while also making it easier for customers to place orders as the company expands.

Other types of considerations that must be taken into consideration as the company expands its credit card transactions to over 1,000,000 a year, would be to increase website security and the accessibility of the website as traffic increases. Even though the S&H Aquarium website will not store customer PII, malicious actors would still be surveilling for flaws to exploit, so S&H Aquarium should take its due care to maintain a secure relationship with its third-party service providers. Network scans would need to become more frequent and at least be performed quarterly. Firewall configuration maintenance and server maintenance and security testing would also need to be routinely performed. The consequences of not increasing website security in tandem with website traffic will result in an unstable cardholder environment that could result in a further increase in merchant level to 1 and penalties from the bank or even the bank ceasing its relationship with S&H Aquariums.

The company will initially accept payments made with MasterCard and Visa only but Discover cards and American Express will be accepted as payment in the future. Discover has the same PCI DSS compliance requirements as Visa and Mastercard, but American Express has stricter requirements. At merchant level 3, American Express only allows 10,000 to 50,000 transactions with its card and 50,000 to 2,500,000 transactions at level 2. As long as there are less than 50,000 American Express transactions and a total of less than 1,000,000 combined Visa, Discover and Mastercard transactions, then S&H Aquariums will remain at level 3. The differences from level 3 to level 2 are still minimal, with American Express only requiring reporting at level 2. However, in addition to the requirements of the other credit cards, American Express, on its site, also requires an External Network Vulnerability Scan, an ASV Scan Report

Attestation of Scan compliance, and an American Express STEP Attestation. This would mean that if S&H Aquariums would like to accept transactions with American Express then they must also build their infrastructure to pass a scan by an Approved Scanning Vendor.

Operating through a hybrid system of e-commerce with a physical location has its fair share of benefits and detriments, but regarding PCI DSS compliance, they have a large overlap. The main concern would have to be the type of PCI DSS SAQ S&H Aquariums will use, in the current and future predictions, the SAQ-A will be filled out. That form of self-assessment questionnaire is for e-commerce merchants that do not store cardholder PII and outsource the storage to a PCI DSS third-party service provider. When S&H Aquariums opens a brick-and-mortar store, then the SAQ would change to SAQ-B because the business is processing cards in-person and online without storing that data. The Point-of-Sale Terminal used to process payments in person also needs to be PCI DSS compliant and the brick-and-mortar store must have its own secure servers and electronic equipment. If the proper form is filled out, and all the equipment that might have information is free from tampering, then there should be minimal issues with PCI DSS compliance in opening a brick-and-mortar store.

Conclusion

Now that S&H Aquariums has a better understanding of the organization’s current and future considerations, the rationale of the importance of the PCI DSS, and an understanding of what PCI DSS is, S&H Aquariums is better positioned to enact policies and implement tools to better protect the cardholder data of the organization’s clients. As the organization grows in size and process volume, the organization is prepared for the increasing amount of compliance standards that it will have to adhere to as it moves to higher merchant levels. Strong security policies, along with well tested tools and systems, will keep the organization compliant and protect the cardholder data of S&H Aquariums and their clients.

References

Chalberg, M. (2019, March 30). *PCI Compliance for Retail Stores: What Every Retailer Needs to Know*. KORONA.Pos. https://koronapos.com/blog/pci-compliance-for-retail-stores/

Kehl, F. (2021, July 12). *The Quick Guide To PCI Compliance For Small Businesses: What You Need To Know & How To Become Compliant*. Merchant Maverick. https://www.merchantmaverick.com/quick-guide-pci-dss-compliance-small-merchants-level-4/

Lumnah, A. (2020, March 27). *A Comprehensive Guide to PCI DSS Merchant Levels*. Semafone. https://semafone.com/blog/a-comprehensive-guide-to-pci-dss-merchant-levels/

PCI Compliance | Keeping Customer Data Safe. (n.d.). Visa. Retrieved August 5, 2021, from https://usa.visa.com/support/small-business/security-compliance.html

Very Good Security. (2019, December 9). *PCI DSS Compliance: A Guide for E-Commerce Businesses | Very Good Security*. Very Good Security - Blog. https://www.verygoodsecurity.com/blog/posts/pci-dss-compliance-a-guide-for-ecommerce-businesses

WooRank. (2018, October 16). *How Does Getting Hacked Affect Your Website or Business?* https://www.woorank.com/en/blog/how-does-getting-hacked-affect-your-website

Kohl, J. (2019, September 7). *5 Consequences to PCI Non-Compliance*. APS PAYMENTS. https://creditcardprocessing.apspayments.com/blog/5-consequences-to-pci-non-compliance

Payment Card Industry Security Standards Council. (2018, May). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*. PCI Security Standards Council. https://www.pcisecuritystandards.org

Wróbel-Konior, S. (2016, August 11). *What is PCI Compliance?* SecurionPay - Payment Platform with Advanced Technology. https://securionpay.com/blog/what-is-pci-compliance/

Wróbel-Konior, S. (2020, February 5). *Why Is PCI Compliance Important for Every Merchant?* SecurionPay - Payment Platform with Advanced Technology. https://securionpay.com/blog/pci-compliance-important-every-merchant/