Introduction to the PCI DSS: What Merchants Need to Know

Successfully managing a business in today's environment is, in its own right, a challenging feat. Uncertain economics, increasing regulatory pressures, and growing competition place enormous stress on business owners. An additional stress, one rarely contemplated even 15 years ago, is the security of consumer data. In the early days of eCommerce, the notion of data compromise was considered, though largely thought to be a concern of large companies with scads of intellectual property to protect. Today merchants are faced with a new reality. Data thefts are an everyday occurrence and its targets are often not the large, household names that one would expect. Small companies often find themselves on the losing end of the data protection battle.

In order to counter the rising number of data thefts, and the increasing number of consumer records compromised by such thefts, the five major card brands (Visa®, MasterCard Worldwide®, American Express®, Discover®, and JCB® developed the Payment Card Industry Data Security Standards, or PCI DSS. The objective was to provide any entity that stores, processes, or transmits cardholder data a baseline of security protocols to implement to more properly protect consumer data. The PCI DSS consists of 12 high-level security requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Figure 1: Payment Card Industry (PCI) Data Security Standard, v3.1© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

Each requirement has a number of sub-requirements that detail the manner in which the security protocol is to be implemented. When totaled, there are now more than 400 PCI DSS requirements and sub-requirements with which merchants must comply. This can be a daunting task, but there are a number of tips that businesses can use to achieve, manage, and validate compliance with the PCI DSS.

Understand Your Data and Your Data Flows

Many businesses have not examined the ways in which data comes into their environment, how it flows through the systems, where it is stored, or with whom it is shared. This is often accompanied by a lack of understanding of what constitutes sensitive data, which, in this case, is cardholder data. This understanding, though, is fundamental to ensuring the protection of data. Without knowing what data is being collected and how, it is not possible to implement controls to protect it.

An excellent starting point is to understand what data is being collected and why. It may be the case that the organization is capable of providing its services without collecting certain types of data. A good guideline is to collect the minimum amount of data needed to fulfill the obligation to the customer. For example, using an end-to-end encryption and tokenization service such as ProtectPay, may be a useful alternative to collecting payment data via web forms and forwarding that data to the payment provider. By using a solution like ProtectPay, the merchant is still able to accept payment via a website without the added burden of having to store, process, or transmit cardholder data.

Further, if it is determined that cardholder data is going to be collected, it is recommended that a data map be created. This map will tell auditors how the data comes into the system and where it goes within that system. Any system that touches cardholder data, or is connected to a system that touches cardholder data, is considered the "Cardholder Data Environment," or CDE. The CDE represents the scope of the environment to which PCI DSS applies.

Knowing the scope of the CDE, and ensuring that it is updated to account for any changes to the environment or data collection process, can help accurately determine how large the compliance project is. Merchants are required to provide the scope of the CDE to their Qualified Security Assessors[1]. Specifically, the PCI DSS states:

"The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. "

Failure to have an accurate scoping document may result in either too broad a scope, or an inadequate assessment of the environment and an erroneous finding of compliance.

Validate Your Service Providers

Many merchants choose to use the services of various technology providers in order to help streamline their business processes. One example of this would be entering an order into a provider's billing software, which can also be used to track inventory and to process payments. From an operational

[1] A Qualified Security Assessor, or QSA, is a professional that has been vetted by the Payment Card Industry Security Standards Council (PCI SSC) to conduct assessments against the PCI DSS. A QSA must work for a company that has been qualified by the PCI SSC.

perspective, such measures are very useful. However, they may also introduce unnecessary risk and jeopardize a merchant's compliance.

A service provider is defined as any entity that stores, processes, or transmits cardholder data on behalf of a merchant or bank. Service providers must be compliant with the PCI DSS and registered with the card brands. Compliance and registration of service providers offers another layer of protection to merchants. If a service provider suffers a breach, and is neither registered nor compliant, the merchant becomes responsible for their affected data. However, if the service provider is compliant and registered, the service provider is ultimately responsible for the breach, rather than the merchants for whom the service provider was handling the cardholder data.

Prior to entering into a contract with a new service provider, merchants should address the issue of PCI DSS compliance. They must ensure that any service provider engaged will offer customer data at least the same level of protection that would be provided by the merchant. PCI DSS Requirements 12.8.5 and 12.9 outline the new PCI requirements with which merchants must comply. Merchants can gain some assurance about the compliance of their service providers by obtain an Attestation of Compliance from them. A list of compliant, registered service providers can be found at http://www.visa.com/splisting/searchGrsp.do.

Compliance is a Year-round Exercise

There is a temptation to manage compliance as a "once a year" task, re-validating compliance on the merchant's anniversary date. However, compliance is much more than a check-box exercise. It requires maintenance on a year-round basis. For example, a merchant that adds new devices or even segments to a network must ensure that those additions do not negatively impact their PCI DSS compliance. Each time a change is made, merchants should evaluate how that change is going to impact its compliance posture. This helps protect the network and saves the organization from unpleasant surprises when it is time to re-validate compliance.

Further, the threat landscape may change significantly in twelve months. New vulnerabilities may be discovered, and new actors may emerge with different motives for data theft and network compromise. Merchants are advised to have a process in place to account for these changes and be able to address them within a reasonable period. Failure to account for new threats may impact a merchant's compliance posture, jeopardize the security of data and ultimately place the organization and its customers at risk.

Lastly, as mentioned earlier, some merchants may be required to submit quarterly vulnerability scans to validate compliance. These quarterly scans are not merely academic exercises for the merchants. They can identify serious vulnerabilities in a merchant's environment. While carrying out these scans on a quarterly basis may be required for compliance, they also support the ongoing attention to security that can help protect customer data.

The PCI DSS is Subject to Change

The nature of the PCI DSS is such that it must evolve. Its objective is the protection of cardholder data. New methods of attack are constantly evolving, as are technologies and business models. The payments landscape can change rapidly, as new technologies and new business models are introduced. The impact of that is that any standard that seeks to address the industry must also change in order to keep pace.

The Payment Card Industry Security Standards Council (PCI SSC), the body responsible for the dissemination and management of the PCI DSS, has published a "lifecycle" timeline.

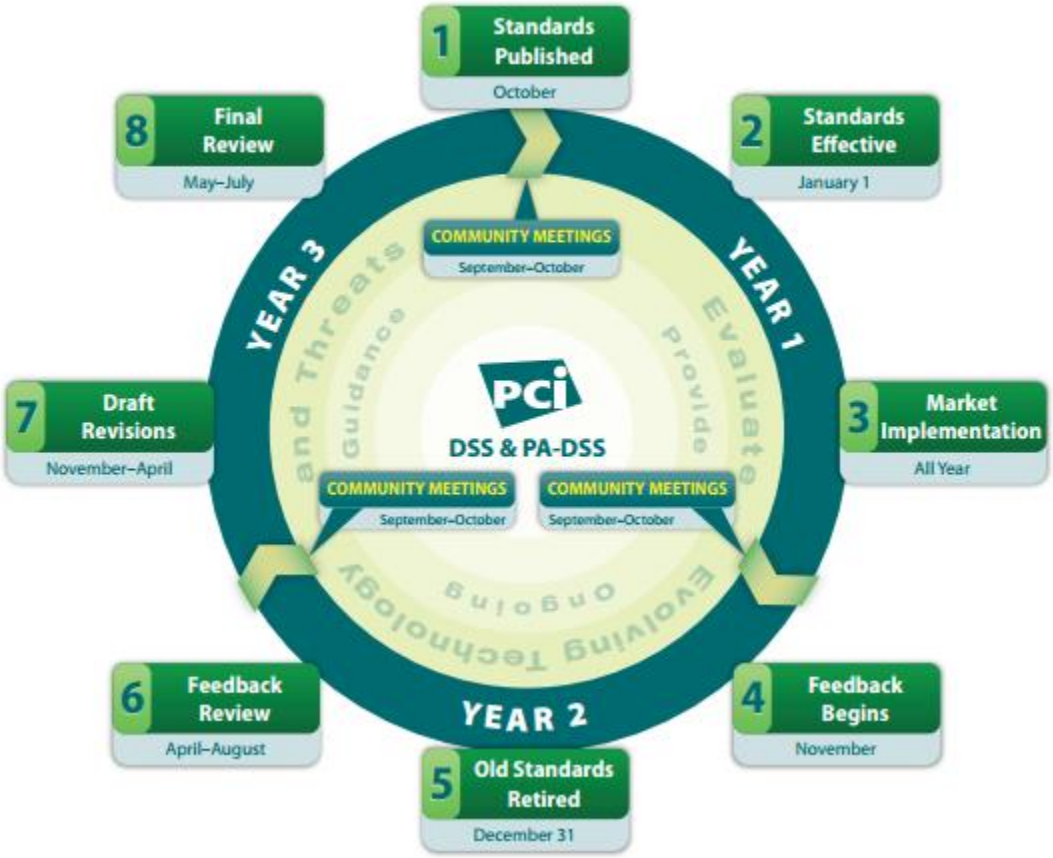

Figure 2: © 2010 PCI Security Standards Council LLC.

In short, the lifecycle is roughly a three-year process, during which time the payments community has the opportunity to provide comment and feedback. The takeaway from the process for merchants is that, in order to remain in compliance with the PCI DSS, the changes in the standard must be monitored.

In addition to the lifecycle of the PCI DSS itself, the PCI SSC often releases guidance documents. These documents are intended to provide supplemental information to the standard or to clarify certain requirements. The Guidance Documents can be a valuable source of information and can assist merchants in preparing for upcoming changes to the standard.

It is vitally important for merchants to stay abreast of the changes to the PCI DSS. Given the rate of change in the standard and the accompanying guidance documents, merchants can find that actions and processes that supported their compliance last year may not be acceptable in subsequent years. Additionally, the PCI SSC may also add or change the Self-Assessment Questionnaires (SAQ) by which merchants validate compliance. For example, in the last iteration of the PCI DSS the PCI SSC created several new questionnaires, including the SAQ A-EP and the SAQ C –VT.

Compliance and Security are Not the Same

It is important to bear in mind that there is a very important difference between compliance and security, though the two are complementary. Adhering to the PCI DSS can certainly help a merchant improve its data security. However, there may be newly evolving threats that are not yet contemplated in the PCI DSS. Merchants are well cautioned to ensure that they are monitoring new developments and addressing them, even if they are not explicitly required for compliance. The PCI DSS document itself cautions that: *"PCI DSS comprises **a minimum set of requirements** for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements." (emphasis added)*[2]

It is possible that a merchant that is compliant with the PCI DSS will have some residual risk that is not covered by the standard. Additionally, merchants sometimes mistake the exercise of validating compliance with actively managing compliance. It is important to remember that validating compliance simply means that at that time, on that day the merchant was compliant. As said previously, managing compliance is an ongoing process, whereas validation is merely a snapshot. It is often the case that actively managing security eases the burden of compliance.

Do Not Store Data That is Not Needed

Hearkening back to the first suggestion of this paper, understanding the data is the key to protecting it. After completing an analysis and inventory of the data within the merchant system, it is prudent to determine what data is really needed in order to provide goods or services to customers. Any data that is not strictly needed should not be retained. A data thief would have little incentive to breach the networks of a merchant that holds no data. In the worst-case scenario, a data thief that did penetrate the network would not be able to abscond with anything valuable.

In addition to the theft-prevention benefit, a merchant that reduces the amount of data stored in its environment can also reduce its compliance burden. As fewer and fewer systems are exposed to

[2] *Payment Card Industry (PCI) Data Security Standard, v3.1 (April 2015) Page 5.*

cardholder data, the scope of the environment that must be validated as compliant is condensed. This measure can reduce the cost of achieving and managing compliance on an ongoing basis.

Conclusion

Compliance with the PCI DSS has become a cost of doing business for many merchants. At the core of the PCI DSS, though, is the obligation to protect cardholder data. To do that, a merchant must have a thorough understanding of the data it collects and why. In establishing prudent partnerships with registered and compliant service providers, merchants can reduce their compliance burden and establish efficient payment processes. At first blush, compliance can seem daunting, but by developing a strong understanding of the objectives of the PCI DSS merchants can successfully manage the requirements of the PCI DSS while maintaining a focus on their business goals.