WHITE PAPER

Preparing for the Evolution: PCI DSS 3.0 and Beyond

Symantec. Confidence in a connected world.

May 2014

CONTENTS

EXECUTIVE SUMMARY

Introduced in 2006, the Payment Card Industry Data Security Standard (PCI DSS) was intended to increase the level of security in the payments ecosystem. In order to do so and to remain relevant, the PCI DSS must meet the constantly changing threats to sensitive payment data. As data thieves and criminals adapt to the standard, the standard must evolve. As stakeholders in the payments ecosystem, organizations that store, process, or transmit payment data must be prepared to adapt their security environments to both the PCI DSS and the ever-changing attack vectors used by data thieves and hackers.

This paper traces the evolution of the standard from its adoption in 2006 until the release of version 3.0 in November 2013. It summarizes the new and updated requirements and analyzes them according to their potential impact on organizations as they work to achieve and maintain compliance. As the PCI DSS is not a static target, some trends and technologies that may drive the next round of changes are discussed. Finally, Symantec offers eight suggestions about how organizations can manage compliance, without losing sight of security.

INTRODUCTION

A cursory review of recent data breaches drives home the importance of vigilant data security practices. In 2013 alone, Privacy Rights Clearinghouse recorded almost 270 incidents of data breach, accounting for more than 45 million records. That total does not include the estimated 120 million compromised records that are now being attributed to major retail breaches that took place in November 2013. That would bring the total number of compromised consumer records in 2013 to almost 170 million.

Almost 170 million

The total number of compromised consumer records in 2013.

As payment channels have proliferated, from traditional eCommerce to cutting-edge mobile payment solutions, the sheer amount of data that is transferred has grown exponentially. For thieves, this means that targets of opportunity abound. Malware that is purposely built to steal data from POS systems is widely available in the underground marketplace. In some attacks, network sniffing tools are used to collect credit card numbers as they traverse internal unencrypted networks. At other times, RAM scraping malware is used to collect credit card numbers as they are read into computer memory. In addition, with the rapid increase in the value of data, criminals are motivated to become ever more creative in the manner in which they steal data. According to an article from InfoSec Institute, data from stolen payment cards can fetch prices ranging from US$20–US$100 per card.

As expected, the well-publicized breaches often resulted in increased attention from politicians and the public. Congress, and specifically Senator Robert Menendez, began calling for increased security requirements for companies accepting payment data. Sen. Menendez has been particularly vocal in demanding new protections, even going so far as to propose that the Federal Trade Commission be authorized to fine for data breaches. Currently, the FTC's involvement in data breaches is in the form of enforcement actions as a result of "unfair or deceptive" trade practices. This increased scrutiny from the public and from politicians makes adherence to standards and best practices more important than ever. The question then becomes how to ensure that the PCI DSS remains relevant in the face of increasingly sophisticated attacks.

EVOLUTION OF THE PCI DSS

The PCI DSS as a standard continues to evolve. That evolution takes into account new technologies and business practices, as well as newly introduced threats. Over the course of its lifespan, the Payment Card Industry Security Standards Council (PCI SSC) has introduced a number of new standards to account for the security of payment applications, end-to-end encryption and tokenization solutions, and mobile payments. In addition, the PCI DSS has undergone a number of revisions to ensure that the standard is relevant to today's environment. The most recent iteration of the PCI DSS, version 3.0, contains a number of changes designed to increase the overall level of protection surrounding cardholder data.

PCI DSS v.3 Updates

Requirement	Update
2.1	The addition of POS terminals and applications will dramatically increase the work effort and expense that organizations must undertake in order to comply.
9.9 (new)	Organizations must maintain an inventory of such devices; periodically inspect POS devices to detect tampering or substitution; and provide training to personnel so they can be aware of attempted tampering or replacement of devices.
8.5.1	This requirement mandates that service providers that have access to the customer environment have unique access credentials.
10.2.5	This requirement for logging access to accounts now includes logging changes to identification and authentication mechanisms.
12.1.1	Requirement 12.1.1 has changed to the previous 12.2 requirement so that now every relevant requirement that requires "daily operational security procedures" has an additional requirement stating that procedures are now mandated.
12.8	Not only applies to service providers "with whom cardholder data is shared" but also to organizations that can impact the security of cardholder data.

The most recent iteration of the PCI DSS, version 3.0, contains a number of changes designed to increase the overall level of protection surrounding cardholder data.

PCI DSS 3.0 includes changes that can affect particular entities seeking to achieve compliance with the standard. For example, changes to PCI DSS requirement 2.1 can have a significant impact on retail organizations. Originally stated as "Always change vendor supplied default and remove or disable unnecessary default accounts before installing them on the network," the updated requirement includes a clarification. It states that "this applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, SNMP community strings, etc." The addition of POS terminals and applications will dramatically increase the work effort and expense that organizations must undertake in order to comply.

Similarly, the addition of requirement 9.9 requires significant resources from entities seeking to achieve compliance. That requirement states: "Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution." This new requirement means that organizations must maintain an inventory of such devices; periodically inspect POS devices to detect tampering or substitution; and provide training to personnel so they can be aware of attempted tampering or replacement of devices.

Two more changes, those in requirements 8.5.1 and 10.2.5, are both in keeping with the PCI SSC's theme of shared responsibility. These requirements address the need for increased vigilance over third-party relationships, as well as oversight of internal parties. Requirement 8.5.1 mandates that service providers that have access to the customer environment have unique access credentials.

Requirement 10.2.5 was enhanced in the latest iteration of the standard. This requirement for logging access to accounts now includes logging changes to identification and authentication mechanisms. That includes the creation of new accounts; elevation of privileges; and all changes, additions, and deletions to accounts with administrative or root access.

PCI DSS requirements 12.1.1 and 12.2 have been updated and reorganized to reflect the importance of daily operational procedures. Requirement 12.1.1 has changed to the previous 12.2 requirement so that now every relevant requirement that requires "daily operational security procedures" has an additional requirement stating that procedures are now mandated.

The realignment of requirements 12.2 and 12.1.1 is expected to increase the detail of procedural documentation and impact the required awareness training but should not involve major upgrades in technology or processes. It requires companies to review their policies and operational procedures against version 3.0 of the PCI DSS to ensure that all requirements that specify procedural documents are addressed.

PCI DSS requirement 12.8 has also been updated to clarify the entities that are required to be considered "in scope" of the PCI DSS and require contractual language. The most significant change is that requirement 12.8 in version 3.0 of the PCI DSS not only applies to service providers "with whom cardholder data is shared" but also to organizations that can impact the security of cardholder data.

Since PCI DSS 1.2, requirement 12.8 has been a challenge for many organizations to meet. With the expansion of 12.8 beyond those with which "cardholder data is shared," it is anticipated that this requirement will create significant challenges for organizations. For example, a third party that cleans the corporate office space may not be "in scope" of requirement 12.8.

On the whole, the changes made to the PCI DSS reflect an attempt to better define how the cardholder data environment is to be scoped, provide a greater level of flexibility to organizations working towards compliance, and emphasize the importance of security awareness and education. Also, when the PCI DSS requires updated practices, organizations must update their policies, procedures, and training accordingly. This exercise in and of itself can prove to be challenging. What's more, as history demonstrates, it is unlikely that PCI DSS 3.0 will remain unchanged.

The PCI DSS is updated on a three-year cycle. Once a new iteration is published, the PCI SSC immediately begins gathering industry feedback and preparing changes to the standard. As the industry embarks on a new cycle, it is already possible to envision possible updates or changes to the standard, based simply on the rapid adoption of new technologies.

Changes made to the PCI DSS reflect an attempt to better define how the cardholder data environment is to be scoped, provide a greater level of flexibility to organizations working towards compliance, and emphasize the importance of security awareness and education.

IMPLICATIONS OF EMERGING TECHNOLOGIES ON PCI DSS

"Chip and PIN" for Fraud Prevention

Perhaps the most prominent payments technology on the horizon within the United States is EMV, also called "chip technology" and most commonly employed in the United Kingdom as "chip and PIN." EMV is often brought to the fore in the aftermath of a data breach and lauded as a solution to the data security vulnerabilities of traditional payments methods. All of the major card brands currently have programs in place to foster the adoption of EMV technology. Visa offers a waiver of PCI DSS compliance validation for merchants that accept more than 75 percent of their transactions through EMV-ready terminals. Further, in 2015 Visa will enact a liability shift to the effect that merchants that are able to accept EMV but instead transact using magnetic stripe will be responsible for fraudulent purchases.

EMV or "Chip and PIN" is often brought to the fore in the aftermath of a data breach and lauded as a solution to the data security vulnerabilities of traditional payments methods.

While EMV certainly does provide some improvement in fraud prevention, the PCI SSC has already publicly stated that the adoption of EMV will not render the PCI DSS obsolete. In 2010, the PCI SSC released a paper on the applicability of the PCI DSS in an EMV environment. It noted: "In the future, should EMV become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence, the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly."

Risk Assessment and Security for Virtualization and Software-Defined Data Centers

Another rapidly evolving technology that will continue to impact the evolution of the PCI DSS is virtualization and the software-defined data center. Virtualization changes the potential attack surface and, if not implemented appropriately, can increase the threat to cardholder data. The hypervisor represents a potential single point of failure. Accordingly, the PCI SSC released an information supplement in 2011 detailing guidelines for implementing virtual environments in the cardholder data environment. The information supplement represents guidelines for implementation but does not constitute a requirement. It is likely, however, that as virtualization and cloud computing continue to gain traction, the PCI SSC will address these technologies in a more formal manner.

PLANNING FOR ADVANCED PERSISTENT THREATS AND THE EVOLVING THREAT LANDSCAPE

As technologies change, so do the threats facing organizations that accept payment cards or handle cardholder data. The most notable new threat is that of advanced persistent threat (APT). APT is defined as a network attack in which the intruder gains access to a network or system, moves laterally through the network to gain access to data, and then slowly exports the data. The hallmark of an APT attack is the length of time in which the attackers stay in the network. It is not uncommon to find APT victims that have been compromised for several years before identification of the attack. The goal of an APT is not to get in and out quickly, but to remain undetected as long as possible to maximize the amount of data acquired.

Given the pace and nature of change, it is a wonder that organizations can address security and compliance. Three years can seem like a sufficient amount of time to prepare for the changes that are likely to come in the next iteration of the PCI DSS. Maintaining compliance and making adjustments may appear to be achievable. Compliance, though, is not security. While compliance is important, it does not guarantee that an organization is impenetrable. In fact, an argument could be made that security is more important than compliance. Compliance should be a byproduct of a strong security foundation, particularly as the PCI DSS continues to evolve.

The goal of an APT is not to get in and out quickly, but to remain undetected as long as possible to maximize the amount of data acquired.

Security is not, and cannot be, static. It must constantly evolve in order to meet the changing threat landscape. While the PCI DSS adapts over a three-year cycle, security threats may emerge overnight. Organizations must be able to react quickly and agilely to newly identified threats. Maintaining a security focus enables a company to protect its data assets and proactively address security. With that in mind, Symantec has identified eight keys to successfully managing PCI DSS compliance and information security in general.

EIGHT KEYS TO SUCCESSFULLY MANAGING PCI DSS COMPLIANCE

1. **Strengthen foundational understanding and organizational capacity.** Having knowledgeable resources that are readily available can make a tremendous difference in an organization's ability to achieve and maintain compliance. Organizations should ensure that their information security teams have the appropriate training and resources necessary to adequately address information security and compliance with the PCI DSS. In some instances, companies may want to engage with outside firms to provide training, awareness, or general consulting to augment the information security capacity of the company.

2. **Do not delay your security and compliance project.** It can seem a daunting task to change a data security or compliance practice to adhere to a new standard. What's more, policies must also be updated and processes defined to meet those new standards. In fact, several of the changes in PCI DSS 3.0 are centered on documentation, policies, and procedures. These updates are often perceived as subordinate to technology implementations, but policy is just as important to compliance as technology. Policy allows companies to create and implement consistent, repeatable processes.

3. **Look beyond the PCI DSS.** Most companies are balancing multiple compliance obligations. While they may seem only distantly related, looking for technologies, processes, and policies that can be extrapolated across the organization can help companies build a cohesive, organic information security governance structure. Such a structure can help organizations achieve and maintain compliance with multiple compliance obligations.

   In addition to looking beyond the PCI DSS in terms of resource allocation, organizations would be well served to recall that the PCI DSS is merely a minimum standard with which companies must comply. In conducting a risk analysis, organizations may identify risks that are not addressed by the PCI DSS. In those instances, it is suggested that companies proactively address those

identified risks even if not required to do so by the PCI DSS. Not doing so may leave them vulnerable to liability in civil actions, as well as enforcement actions by government agencies such as the FTC.

4. **Identify ways to gain efficiencies.** In addition to looking for ways to leverage technology across the environment, companies may also find ways to reduce costs by outsourcing certain tasks. Small and midsize businesses in particular often struggle with PCI DSS compliance. One option may be to outsource the management of technology to a PCI DSS validated third party. While it may seem counterintuitive that outsourcing can save money, the fact is that the cost of creating or acquiring the internal resources necessary to successfully manage the resources in-house may far exceed the cost of outsourcing.

5. **Leverage tools and automation.** Many companies are using manual processes to manage security, which can leave them with significant exposures. While no one technology can achieve compliance, organizations that find the right mix of manual processes and automated tools can make great strides in managing their compliance on an ongoing basis. Automation is particularly beneficial when considering the use of layered security strategies. As environments grow more complex, the ability to manage the layers of security tools, not to mention the administrative and operational tools that are in place, in the corporate environment gains importance for both security and operational efficiencies.

6. **Maintain proactive security awareness.** Companies that constantly monitor their own environments as attack trends change can proactively address security concerns before they become compliance requirements. In identifying and mitigating new threats, businesses can find themselves well positioned to address changes to the PCI DSS. This proactive approach can also help to mitigate the damage in the event that the organization does suffer a breach. Recent headlines highlight organizations that were breached for months and, in some cases, years prior to the discovery of a data compromise. Being proactive in security may allow companies to more quickly identify a breach, address the issue, and remediate the vulnerability. Such an approach may result in a dramatic decrease in the magnitude of the breach, the damage to the organization, and ultimately the impact on the customer.

7. **Balance security with business objectives.** Oftentimes, information security seems at odds with the “business.” An old adage in security states that all risk can be eliminated if no business needs to get done. The job of security is ultimately to support the objectives of the business. That means finding a way to support business objectives, while maintaining a secure environment. It also means that an open dialogue must exist between the business group and the information security group. With the understanding that the viability of the company may depend on its information security, many companies actively work to eliminate the perceived opposition of the two groups and create a more symbiotic relationship. Bringing information security to the table in business discussions can help create a collegial atmosphere in which information security becomes a part of the decision-making process.

What's more, as consumers become more wary of sharing their sensitive data, compliance with the PCI DSS can become more than simply an industry mandate or a self-protective measure. Security, as well as compliance, can become a competitive advantage. eCommerce retailers often highlight their security and privacy protections to put customers at ease. While security and privacy statements can help convert customers, it is important that there be substance to these statements.

8. **Make compliance a way of life.** Compliance as an afterthought is an ineffective way to maintain adherence to industry or regulatory standards. The PCI DSS mandates training and awareness of employees on information security and compliance. If the only departments aware of the duties of the company to protect data are the compliance and information security groups, it is safe to assume that the company is not compliant. Training all employees in their roles in data protection can significantly enhance the compliance posture of the company. Further, employees that are empowered to report potential instances of noncompliance or areas of concern can help a company proactively address issues, before a breach occurs. Companies are also able to embed compliance in the organizational fabric, as well as balance security with operational objectives, by using automation and risk analysis to align compliance with security and IT operational priorities. Companies will always face multiple conflicting urgencies. A risk-prioritized approach to compliance and security remediation enables them to optimize their resource allocation.

CONCLUSION

The PCI DSS is not a static target, nor should it be. Its purpose is the protection of cardholder data, and it must constantly evolve in order to support that purpose. PCI DSS compliance is not a singular endeavor for businesses to consider once per year. It is an ongoing process. Companies that have a strong security foundation are best positioned to comply with new requirements.

Data has increasingly become the fuel for business engines. However, the more data stored, the greater the challenge of protecting that data. Using information security tools that work together seamlessly has become mission critical. Organizations seeking to balance business objectives with security and compliance requirements would be well served to seek out security partners with a breadth of products and experience to help manage the ever increasing strain on the organization.

Symantec's industry-leading position as a security expert means that is uniquely qualified to help companies meet the unique demands of both information security and compliance. A veteran of more than 25 years in the field of IT security, Symantec counts the payment card industry's large retailers, banks, telecommunications firms, and service providers among its most valued clients. Symantec's industry-leading security, data protection, and management products and services provide excellent coverage of the PCI DSS requirements. As both a Qualified Security Assessor and an Approved Scanning Vendor, the Symantec Consulting Services organization combines technical expertise and methodologies with practical experience.

Symantec Confidence in a connected world.

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com