

Payment Card Industry (PCI) Data Security Standard (DSS)

“Embracing PCI – Making it work for you”

Executive Summary

With the recent rise in data breaches and identity thefts, implementing a sound information security program is no longer optional. Companies processing credit card information are encouraged to embrace and implement sound data protection strategies to protect the confidentiality and integrity of payment information. As a result of this recent trend, a consortium of payment card providers collaborated to introduce the Payment Card Industry (PCI) Data Security Standard (DSS) to ensure that companies take due care and diligence in storing, processing and transmitting credit card data. The goal of PCI is to improve data protection strategies that will allow consumers to swipe their credit cards with more confidence and assurance that the confidentiality and integrity of their information will not be compromised.


Some of the challenges for achieving PCI compliance are outlined in this white paper, as well as successful tips to help organizations navigate through these challenges. Although challenges exist, organizations should remain encouraged and focused because there are benefits for achieving PCI compliance as outlined in this white paper. By achieving PCI compliance organizations eliminate unnecessary fines and penalties, heighten the awareness of PCI standards and requirements, and assist in the preparedness and readiness for upcoming PCI assessments and audits.

This white paper provides guidance on how to achieve PCI compliance and a summary analysis of the 12 security requirements of the PCI security standard. A good first step toward achieving PCI compliance is embracing it while realizing no standard is perfect. The key to embracing PCI and achieving compliance is to understand that at the “heart” of the PCI standard are sound, fundamental security practices for data protection that seek to protect data confidentiality and integrity. One of the keys to understanding PCI is realizing that it’s not a security panacea, but rather the starting point to help organizations put in place a process for implementing and regularly reviewing sound information security principles for data protection. Thus, making PCI work resides in your ability to seamlessly align and integrate PCI with your existing information security policies, procedures, standards and guidelines.

About the Author

Kevin E. Greene is a Sr. Security Consultant for Dickerson Technologies. Kevin has over 10 years of experience in Information Security and Information Assurance and has written and contributed to numerous publications and white papers on various Information Security topics. Kevin holds a Master’s and Bachelor Degree from New Jersey Institute of Technology (NJIT) and is currently an active member of Information Systems Security Association (ISSA) for information professionals and practitioners.

Over the last 10 years, Kevin has been actively working with clients in developing and formalizing their compliance strategies



to meet PCI, Sarbanes Oxley (SOX), and Health Insurance Portability and Accountability Act (HIPAA) requirements for ensuring data confidentiality and integrity. In most recent years, Kevin has been engaged in various projects assisting federal agencies with their Certification and Accreditation (C&A) process, including documenting, validating and testing security controls. In addition, Kevin has been working with various security vendors in developing data protection strategies and solution offerings that provide not only data protection, but also a framework that leverages sound information assurance principles.

Introduction

The threats to sensitive and confidential data are consistently on the rise and consumers are becoming less confident that their data and identity can be protected. The U.S. Federal Trade Commission (FTC) received over 670,000 complaints in 2006 — of which 36% were identity theft complaints and 64% were related to other types of fraud. In 2005, over 680,000 complaints and in 2004, over 650,000 complaints were reported. In the Consumer Sentinel report it goes on to reveal that over 35% of the complaints were identity related and over 60% of the complaints were fraud related over two years spanning from 2004 to 2006. These numbers give us clear indications that protecting sensitive information, in particular credit card and payment information is increasingly important. Many of these cases were a result of data breaches associated with credit cards. Therefore, the credit card companies had to act. So a federation of companies, such as MasterCard, VISA, American Express, Discover and JCB, set out to establish consistent data security measures for merchants, banks and service providers. Thus Payment Card Industry (PCI) Data Security Standard (DSS) came to fruition in 2005 and was later revised in September 2006 to provide guidance for protecting credit card and payment information.

Embracing PCI

So, it's safe to say that PCI is here to stay, at least for the foreseeable future. If you are an industry participant or entity that stores, processes or transmits cardholder information, I have a newflash for you — “Embrace PCI” . . . and make it work for you. The guidance that PCI DSS provides is the starting point to get organizations (back) on the right track toward compliance, improving data protection strategies, and adopting a holistic and comprehensive approach to information security. This will ultimately help reduce fraud and inject more confidence in the global credit issuance industry. This is positive news, which one would think should be received in a positive light; however, there are many who would argue that PCI is not realistic or attainable. There are quiet whispers for a more lenient and cost-effective approach — the microwave approach to information security and assurance.

The guidance that PCI DSS provides is the starting point to get organizations (back) on the right track toward compliance, improving data protection strategies, and adopting a holistic and comprehensive approach to information security.

PCI DSS consists of 12 major security requirements which provide some level of guidance for protecting payment information. These requirements encourage industry participants to develop, implement and maintain fundamental security practices to establish the necessary framework for sound data protection strategies. One should keep in mind that the guidance provided by PCI DSS contains basic requirements that are often incorporated into the fabric of traditional Infor-

mation Security and Assurance programs. Therefore organizations that are diligent and serious about information security and assurance should be ahead of the game in achieving compliance {PCI, HIPAA, FISMA, SOX}. However, the problem for many industry participants, partners and merchants is that PCI DSS is all there is to their Information Security and Assurance

PCI is...not an end-all, be-all check list or a replacement for a corporate information security strategy as many companies have been regarding it.

program — and many are not taking the proper steps to protect their payment information. Essentially, they don't take PCI DSS far enough by incorporating it as part of a larger, continuous process to validate and measure their basic and fundamental security practices. In other words, PCI is not a security panacea — it's not an end-all, be-all check list or a replacement for a corporate information security strategy as many companies have been regarding it. This fundamental flaw in how to use this standard has led to the current perception of PCI DSS — if PCI DSS is merely a replacement for a well thought out Information Security and Assurance program tailored for a company, it's conceivable to feel or believe that achieving compliance is not realistic, attainable or cost-effective. That is because too often the approach for implementing effective and sound information security practices is merely focused on getting a passing grade on their scorecard. Security practices are not well planned, are often poorly budgeted with misplaced emphasis, and are very reactive in nature, too network-centric, unbalanced, and non-strategic. There must be a method to the madness. That is to say, organizations have to work diligently to improve overall planning, budgeting, and strategy, and this in turn will help organizations to more easily achieve compliance for not only PCI, but other standards as well.

program — and many are not taking the proper steps to protect their payment information. Essentially, they don't take PCI DSS far enough by incorporating it as part of a larger, continuous process to validate and

PCI Challenges

So is achieving PCI compliance realistic, attainable and cost-effective? The answer is absolutely, Yes! One of the first things that organizations need to do is demystify the myths about PCI compliance that will ultimately help reposition their perspective and redefine their approach to information security and assurance. In doing so, organizations will fully understand that PCI by itself can marginally improve security because a PCI assessment will only provide a snapshot of an organization's security posture and not a comprehensive or holistic view of the deficiencies that may exist. Thus, organizations should be cautioned not to become complacent in thinking that the work is over. The threat landscape is constantly evolving; threats are becoming more complex, stealthier and more innovative, and data and information is much more accessible. Therefore it's important to view PCI compliance as part of a continuous security improvement process and not a check-list exercise.

A Closer look at PCI

There are essentially 12 security requirements highlighted in the PCI standard

- Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus

Requirement 6: Develop and maintain secure systems and applications

- Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

- Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

- Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Understanding PCI

The 12 security requirements outlined by PCI DSS will require technology products and solutions to be implemented in the enterprise for compliance. If you look at each of the 12 requirements, several technology products and solutions immediately come to mind including (but not limited to): Application Firewall, Data Leakage (DLP), Configuration and Audit Control, Identity and Access Management (IAM), Encryption software, Security Information Event Management (SIEM), Intrusion Detection/Prevention solutions (IDS and IPS). Typically that's how deficiencies, vulnerabilities, security exposures and risks are addressed and mitigated, by relying heavily on technology to be the end-all, be-all approach. It's easy to get caught up in buying and spending money on technology products and solutions, rather than focusing on implementing sound processes and comprehensive policies to provide a continuous and consistent framework that will ultimately govern how technology will be implemented in the enterprise.

Often many IT security professionals (and even some auditors) misinterpret security and compliance guidance handed down by various governing entities which often lead to an implement technology first approach, rather than doing an assessment and gap analysis. It is important to fully understand that there's no "one size fits all" solution that exists to achieve PCI compliance. An assessment and gap analysis will provide organizations an opportunity to identify commensurate controls for achieving PCI compliance. After these controls have been identified, organizations can begin outlining a plan of action and strategy for implementing controls - Technical, Operational and Management. The plan of action and strategy should prioritize which controls are least and most likely to be implemented, as well as any compensating control deemed commensurate to mitigating risk. It has been widely speculated that many organizations are underestimating the associated costs for PCI compliance. Achieving PCI compliance can be a huge cost undertaking (depending on your overall security posture); however, by prioritizing, organizations can determine how much PCI is going to cost. In many cases, costs can often dictate and drive what security controls are going to be implemented. Be mindful that the cost of not being PCI compliant in terms of fines, loss of public confidence and business impact can far outweigh the cost of achieving PCI compliance.

Making PCI work for you

Here are some tips and insight that can help you better interpret PCI guidance.

Requirement 1 - Install and maintain a firewall configuration to protect cardholder data

Summary: Does this really mean going out and buying a new firewall and installing it? It depends. It may make more sense to implement a new firewall if you haven't kept up with the latest technologies because firewall technologies have improved quite a bit over time. The concept of "firewalling" through network segmentation isolates payment processing systems from the rest of the network, limiting the scope of PCI to only those systems that process payment information, and not the entire network. Although not required by PCI until June 2008, using a "web" application firewall can offer much more control through tighter policy enforcement, specific application protection, and visibility into network traffic to detect and mitigate new threats as they emerge.

This requirement is also focused on ensuring that there are established processes and procedures in place for sound

firewall management, deployment, operation, and maintenance practices. There should also be an established process and/or procedure in place to audit and review the firewall configuration on a consistent basis.

PCI Smarts - *A Firewall policy should map back to a “Corporate Security Policy” that validates and identifies what traffic is allowed in and out of the network.*

Requirement 2 – Do not use vendor supplied defaults for systems passwords and other security parameters

Summary: Develop a password policy that is enforceable and auditable. . . There should be a “configuration standard” or hardening guide for all systems {servers, firewalls, routers} outlining the procedures for changing default passwords on systems and using stronger authentication mechanisms to meet password and authentication policies established within the organization. Overall password management has always been one of the hardest things for organizations to wrap their arms around. Implementing an identity-based solution can yield great returns, while improving password security. The goal is to maintain a high-level of assurance that users can be properly identified, authenticated, and authorized to access key systems and services on the network.

PCI Smarts - *One way to improve overall password management is to leverage directory and identity based services on the network. If there is a need for stronger authentication, one should consider two-factor authentication solutions that can integrate with directory and identify based services.*

Requirement 3 – Protect stored cardholder data

Summary: Protecting stored payment information is becoming increasingly important and many are considering implementing some form of data encryption to protect stored data (data at rest).

This requirement becomes a bit more challenging for many reasons:

- Data Is Everywhere — it’s difficult to protect data when you don’t know where the data resides.
- Systems with payment card information are not properly classified.
- There are challenges in implementing enterprise-wide encryption and determining what solution best fits your business needs and technical requirements.
- Data retention policies are often inconsistent.
- Database security standards and hardening guidelines are often ignored.

Requirement 4 – Encrypt transmission of cardholder data across open, public networks

Summary: SSL for web traffic, SSL VPN for remote access solutions, Email encryption (TLS, S/MIME, PGP or desktop-to-desktop) and IPSec VPN to protect the confidentiality of payment card information.

One of the exposures and vulnerabilities not explicitly covered in PCI DSS is data leakage, which is unauthorized transmission of cardholder data via Instant Messaging (IM), email (attachments), FTP and other file sharing applications/protocols (often known as data in motion). In order for PCI to be effective, there must be explicit provisions and guidance in

the PCI DSS to mitigate data leakage vulnerabilities and risks. There are industry security solutions designed to detect sensitive information as it leaves the network — Content Monitoring Filter/Data Loss Prevention technology. In addition, it is equally important to not only encrypt data transmission for confidentiality, but also provide visibility into the SSL traffic to detect threats. Organizations should consider implementing web gateway solutions that offer SSL scanning and policy enforcement (confidential documents, credit card and social security number detection) for encrypted traffic. These are becoming attractive solutions for many organizations to secure VPN and remote connections. Messaging encryption is also essential and can be accomplished with either network layer protocol encryption (like TLS) or by encrypting emails directly to the end user desktop.

Requirement 5 – Use and regularly update anti-virus software and programs

Summary: One of the shortcomings of anti-virus is that it's a “reactive” solution that provides limited protection against threats that are stealthier, more innovative and sophisticated. In today's environment, spyware is the new virus without the fame... but with the fortune. Investing in an endpoint solution that employs various detection mechanisms {intrusion detection/prevention (IDS and IPS), application filtering, firewall, anti-spam, anti-spyware and anti-virus} is probably the way to go to protect against malicious threats that seek to steal and leak data. One should consider some flavor of Network Admission Control (NAC) to validate the security posture of endpoints before allowing them onto the network, as well as Unified Threat Management (UTM) and web gateway solutions to offer best-of-breed and in-depth security to mitigate not only viruses, but advanced malware and spyware found in today's Web 2.0 applications. Spam is often the carrier of inborn threats and strong anti-spam prevention methods will go a long way toward preventing malware infections.

PCI Smarts - *In dealing with today's threat environment, leveraging both a “reactive” (signature-based) and “proactive” (reputation-based intelligence) approach will help improve overall detection capabilities, response capabilities, remediation planning, policy enforcement and assessment of risks in the computing environment.*

Requirement 6 - Develop and maintain secure systems and applications

Summary: Use existing application and operating system industry “best practice” guidelines as a starting point to create and develop your own security standards. Take those standards and tailor them to your existing environment to meet your needs. In addition, validate that standards and patch management are adhered to by conducting routine scans to identify deviations from baselines. In June of 2008, implementing a “web” application firewall will evolve into a requirement, so now is the time to start evaluating application layer firewalls that can protect your environment from some of the more sophisticated attacks like SQL and cookie injection, unknown zero-day web worms, XML and SOAP attacks, and cross-site scripting attacks to name a few. It is also important to be able to enforce SSL scanning on encrypted traffic before it reaches the web application to detect potential attacks that may be embedded in the SSL traffic.

PCI Smarts - *Often security professionals spend most of their time retrofitting security into applications. Many of the flaws in poorly written application/code occur because there is no consistent System Develop Life Cycle (SDLC) process in place that incorporates sound and fundamental security practices and principles.*

Requirement 7 – Restrict access to cardholder data by business need-to-know

Summary: : Access in critical network environments begins with proof of identity. Only properly authenticated, properly authorized individuals should be allowed access to the network. An access control system that integrates tightly with an Identity and Access Management (IAM) system should be used to enforce this requirement. Additionally, application and user accounts should be audited on a regular basis to determine if roles and systems are still current and accurate.

Requirement 8 - Assign a unique ID to each person with computer access

Summary: Implementing and enforcing password policies. A process should be in place to audit user account management on a consistent basis to identify anomalies. If at all possible, automate as much of the user provisioning process as possible to improve user account management. This section of the standard specifically requires the implementation of two-factor authentication. Two-factor authentication will ensure that user accounts are not shared amongst users and thus requires organizations to assign a unique account to each computer user. Additionally, two factor authentication will ensure that audit records accurately depict who accessed what systems and when. This will help identify the responsible party in the event of a data breach. Identity and Access Management (IAM) becomes the perfect solution to seamlessly integrate access requirements, improve management and provide identity-based services.

PCI Smarts - Security Awareness training (employee orientation) can be used to educate users regarding password policy. In addition, creating synergies between Human Resources and IT (specifically the Help Desk) is a key aspect of the user provision and account management process. The HR department has a consistent pulse on employment status.

Requirement 9 – Restrict physical access to cardholder data

Summary: Any physical access to data or systems that house cardholder data should be restricted. If I can gain unauthorized access by walking up to a server and remove a tape drive (media drive) that has cardholder data, it defeats the purpose of having logical security controls in place. So... it's important to develop sound processes and procedures for physical security and facility access to limit and monitor authorized and unauthorized access to systems. Often data center and server room security is lax; there are no visitor escorts, visitor badging, or sign-in sheets, and server racks are left unlocked and unattended.

Requirement 10 – Track and monitor all access to network resources and cardholder data

Summary: Logging and audit trails are essential pieces of information to determine security breaches, to identify security anomalies and abnormal user and network behavior. The problem is that systems and network devices provide a wealth of log data and it becomes difficult to sift through the volumes of it. Data normalization, mining and correlation are key elements to any log management system, as well as forensic tools for incident response. Security Information Event Management (SIEM) tools are the best solutions today to meet this monitoring, mining and reporting requirement.

PCI Smarts - Event correlation and normalization through Security Information Event Management (SIEM) tools reduce and ease the burden of sifting through logs to pinpoint “interesting” events. Although not explicitly stated, network-based and host-based Intrusion Detection/Prevention (IDS and IPS) tools are key tools to consider implementing for visibility into threat activity.

Requirement 11 – Regularly test security systems and processes

Summary: Conducting a quarterly security audit (by a third-party) is a good practice. Discovering vulnerabilities, weak controls and security deficiencies is definitely the goal. However, ensuring that there are sound processes in place for patching, SDLC, configuration management, code review, change management is critically more important for a number of reasons, mainly zero-day exploits. Regular security testing is a good practice to incorporate for validation, rather than discovery.

Requirement 12 – Maintain a policy that addresses information security for employees and contractors

Summary: This is as fundamental as you can get. Without an actionable security policy that’s communicated and enforceable, the guidance provided in requirements 1-11 are completely useless. Incorporating aspects of information security into the overall culture is important. Users and employees often view “security” as change or a hassle, and often resist, so clear communication is paramount for success. This requirement should be the first requirement listed in PCI DSS.

PCI and beyond

One of the major hurdles toward achieving PCI compliance is the juggling act that seeks to mitigate risks without extraordinary expenses and without affecting performance and productivity. Keep in mind that PCI has to be tailored for your organization based on the strengths and weaknesses of your Information Security and Assurance program. Obviously, if you have a mature Information Security and Assurance program most of the guidance covered in PCI DSS would already be established and incorporated. PCI DSS interpretation is very important in developing your strategies for PCI compliance. Explore all your options; seek help from security experts to navigate through PCI DSS. Consider the following recommendations to get you started toward PCI compliance:

1. **Perform an audit of your network and security infrastructure.**
2. **Identify and classify your data so that you can implement the proper controls for protection.**
3. **Protect the confidentiality and integrity of data in motion and at rest.**
4. **Consistently monitor access to your data by enforcing logging and audit trails. Limit access to sensitive and critical data to only a “need to know” basis.**
5. **Continuous monitoring improvement – keep a pulse on the security threats in your environment.**

With the heightened awareness recently focusing on improved data protection strategies to prevent data loss, PCI compliance emerges as a vehicle that many organizations can use to arrive at their destination. This will allow consumers to swipe their credit cards with more confidence and assurance that the confidentiality and integrity of their information will not be compromised. As industry best practices and standards for data protection continue to evolve, PCI will likely

become more comprehensive in scope to expand beyond the 12 security requirements. There's already plenty of buzz in the industry about the revised PCI DSS standard due by the end of 2008. Much of this buzz regarding the new PCI DSS revision calls for improved and enhanced web-application security, which has been increasingly under the microscope in the larger security community. The details about the new revisions at this point are still hearsay, but brace yourself and keep a watchful eye on the PCI DSS developments, as they are set to evolve imminently before our eyes in 2008.

About Dickerson Technologies

DICKERSON TECHNOLOGY LLC is a privately held full service Information Technology consultant firm who specialized in LAN/WAN administration, Information Assurance, Network Security, and Information Security Research. Founded in 2002 specifically to expand the awareness of security issues in Information Technology, the company provides state of the art solutions to mission critical applications and vital organizations. The company represents more than 40 person-years experience, having been involved in the initial development and implementation of a range of IT security technologies like virus and malware protection, encryption, firewalls, intrusion detection, and Virtual Private Networks (VPNs).

We offer a wide range of Information Security and Assurance services to assess, identify, mitigate and manage risk in the business environment. Our Information Security and Assurance services assist organizations in establishing a solid security framework that integrates policy, process, technology and people to create a consistent and holistic approach to protecting critical business assets.

About Secure Computing

SECURE COMPUTING CORPORATION (NASDAQ:SCUR), a leading provider of enterprise gateway security, delivers a comprehensive set of solutions that help customers protect their critical Web, email and network assets. Over half the Fortune 50 and Fortune 500 are part of our more than 20,000 global customers in 106 countries, supported by a worldwide network of more than 2,000 partners. The company is headquartered in San Jose, Calif., and has offices worldwide.

For more information about Secure Computing's products, please visit their web site at www.securecomputing.com.



www.dickersontech.com



www.securecomputing.com