Data Loss Prevention Best Practices to comply with PCI-DSS

An Executive Guide

Four steps for success

Implementing a Data Loss Prevention solution to address PCI requirements may be broken into four key phases which are described in this guide:

- Understand PCI Regulations and DLP Technology
- Establish Priorities with Stakeholders
- Evaluate Alternatives
- Deploy with an Iterative Methodology

What is PCI-DSS?

The Payment Card Industry Data Security Standard, PCI DSS, is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM and POS cards.

The standards cover everything from the point of entry of card data into a system, to how the data is processed by merchants, processors, financial institutions, and any other organizations that store, process, and transmit cardholder data, around the world.

The standards are developed, managed and maintained by the PCI Security Standards Council a global forum founded by five global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. – who have incorporated the PCI DSS as the technical requirements for their data security compliance programs. The Council does not validate or enforce any organization's compliance with its PCI Security Standards, nor does it impose penalties for non-compliance. These areas are governed by the payment brands mentioned above and their partners .

Here PCI data generally refers to Personal Account Number, name and address and other data that may be collected as part of a financial transaction in the course of a retail or other type of sale.

A particular enterprise could have additional sensitive information management concerns For instance, health care companies need to meet the rules and regulations proscribed by HIPAA and its extensions. However, to maintain the stated focus of this paper, such additional requirements will not be addressed here.

The Payment Card Industry Data Security Standard, PCI DSS, is a proprietary information security standard for organizations that handle cardholder information

Understanding Compliance and Risks

The PCI standards impose and define 12 core requirements and an associated roughly 250 controls. These may be summarized into three mainconcerns:

- Any merchant handling payment card information must comply with PCI-DSS.
- A Merchant must not store the card's three or four-digit security code (CVV), the track data from the magnetic strip or the PIN data
- A merchant must meet certain security requirements if PCI data is passing through or being stored there.

To demonstrate PCI compliance merchants need to complete a Self-Assessment Questionnaire (SAQ), a compliance validation tool. The versions of this tool are aimed at trying to accommodate different business types and processing methods. Large merchants may need to have an Assessment performed by an outside organization that has been qualified by the PCI Council.

The improper release of regulated personal financial data can result in painful consequences to the organization(s) responsible - ranging from damaging media exposure to harsh fines for serious incidents.

A proper Data Loss Prevention, DLP, technology when implemented appropriately will greatly assist in compliance with the PCI standards and significantly reduce the risks of a PCI data breach.

Understanding What is DLP?

Data Loss Prevention, DLP, refers to technology employed for the purpose of reducing the risks from loss of control over sensitive data. Not all DLP offerings on the market are equal, however. Because of its unique advantages and powerful capabilities, DLP, here, will be taken to mean "Content Aware DLP" which is often referred to as "Enterprise DLP". Gartner, Inc. provides this definition in its IT Glossary:

"Content-aware data loss prevention (DLP) tools enable the dynamic application of policy based on the content and context at the time of an operation. These tools are used to address the risk of inadvertent or accidental leaks, or exposure of sensitive enterprise information outside authorized channels, using monitoring, filtering, blocking and remediation features."

The improper release of regulated personal financial data can result in painful consequences to the organization responsible.

How Does DLP Help?

The PCI standards 12 core requirements include four (4) that can be addressed by a employing a variety of DLP capabilities:

Standard	Requirement	DLP Services
3	Protect stored cardholder data	A proper DLP Discovery tool will accurately locate unencrypted PCI wherever it resides, DLP processes guide users to automatically encrypt the information, remove the information or other remediation according to the defined policies of the organization
4	Encrypt transmission of cardholder data across open, public networks.	DLP Network tools identify and encrypt any unencrypted PCI before it may be sent outside the organization to a public network.
7	Restrict access to cardholder data by business need-to-know.	DLP accurately identifies all file shares containing unencrypted PCI. Unauthorized access may be remediated by encrypting or moving the data to an appropriate storage with correct access controls.
11	Regularly test security systems and processes.	Continuous DLP Discovery scanning may be applied at desired frequency or on demand to audit security status and maintain awareness of PCI data locations. DLP Endpoint will control the copying of unencrypted PCI on connected devices.

A proper DLP Discovery tool will accurately locate unencrypted PCI data wherever it resides

Planning Requires Representation of All Stakeholders

Selected stakeholders within the organization need to be involved in order to provide sufficient knowledge of the organization's:

- PCI compliance requirements,
- Current Policies relating to handling sensitive information,
- Present information storage and handling processes,
- Information Technology assets

This knowledge will typically require input from:

- Selected Executives
- Compliance and Privacy Executives,
- HR
- IT Security
- Administrative management, and
- Third party consultants specializing in DLP

While many individuals and groups may be involved, one person should be designated with coordinating authority and ownership of the project.

It is important to gain the highest appropriate executive level commitment for this effort. This leadership will be needed as conflicts may arise during the final stages of decisions and as implementation will enforce changes in system user behavior. For example, often individuals are slow to accept changes that are of crucial importance to the organization.

Establish Objectives and Priorities

Whether the organization is evaluating the implementation of DLP for the first time, or wants to audit its already existing systems, it is essential to develop an agreement on what the solution should accomplish is essential. DLP will meaningfully reduce the risk of loss of PCI data across many potential channels. It is critical to set a priority around network loss, endpoint loss or loss due to a file exposed on a shared file system

In establishing these objectives it is important to keep in mind that DLP does not solve every security issue. But it should be a key component of managing the organization's overall security strategy and information governance. In other words, attempting to remove all risk is not a reasonable goal. A fair objective should be to reduce risk to a reasonable level based on the estimated costs and benefits. .

Easy steps should be identified for implementation first. Simple data loss prevention policies will yield very high returns very quickly. Some examples are discussed below.

One person should be designated with coordinating authority and ownership of the project.

Identify Requirements Tangential to PCI

In the process of planning the protection of customer PCI data, the requirements for other, related, sensitive information may be considered and prioritized at the appropriate level. Examples could include data regarding VIP customers such as politicians, well-known figures in the community, professional sports team members, Hollywood stars, VIP children, or unique other extremely sensitive individuals demanding certain of their information be protected.

Identify the Unique Risks from Newer Technology

Gather and review policies and procedures concerning current or planned new technology areas of likely leakage concern. Establishing detailed plans in each of these areas should be developed carefully and with expert advice.

Mobile devices
Smart phones, tablets and various other communicating devices are convenient, growing in popularity and may at times be disconnected from the rest of the system. Moreover, using personal mobile devices for business purposes is a trend with momentum that will continue to grow. Being able to monitor and control any PCI data being sent to and received by these devices is mandatory in today's computing environment.

Cloud storage
The Cloud is increasingly under consideration for possible cost savings and expansion flexibility. With the different sort of risks it embodies this technology should be included in any discussions of plans for managing protected information. This should include the possibilities of both off and on-premise cloud use, as well as the possibility of an individual in the organization storing PCI records on a personal cloud.

Select Modular Solutions with Appropriate Costs

Avoid buying features you will never use. Seek a solution that is modular enough to provide what is needed and does not include unnecessary features (and costs) before they are useful. This means to look for an Enterprise DLP suite with multiple modules that can be purchased one at a time and yet allow consistent policies to be applied across the File Stores, Network or Endpoints, Avoid narrowly focused "solutions" that will address only a single channel, such as email, yet leave the organization exposed to leakage through other paths.

A 5 year Total Cost of Ownership (TCO) analysis should be developed at this point. This analysis should show the monthly, annual and total costs for:

- Hardware,
- Software,
- Maintenance
- Training
- Professional services.

Seek a solution that is modular enough to provide what is needed and does not include unnecessary features and costs before they are useful

Developing a TCO will require understanding the licensing policies of any vendor being considered Determine if the software licenses will be purchased or must be paid for on an annual or monthly basis.

Select Vendors and Consultants With Demonstrable Expertise and Experience

Ask questions in order to understand any vendor's or a consultant's specific experience with PCI requirements and successful prior implementations. Some DLP solution providers use overly complicated polices. Others may rely on overly simple processes that must be tuned considerably before use in certain environments.

Insist on a Proof of Concept demonstration done in your own environment with your own data. Evaluate potential solutions based around how easy is the demonstration to set up and manage. Relying too heavily on "out of the box" solutions is likely to produce an unsatisfactory number of false alarms in practice.

Note that DLP serves a very different purpose than a firewall or mere encryption. DLP effectively combines business process, data and security. A firewall has many standard policies that all organizations should simply enable without tailoring a unique purpose.

Deploy with an Iterative Metodology

DLP is a management tool that will be most effective when applied in iterative stages. This means identifying easily won objectives and accomplishing those. Then assimilating what was learned and moving to the next goal.

Following such an outline will make the DLP implementation less disruptive for both thoseaffected and thoseresponsible for making it work. Progress will be easier to measure and the course easier to alter when needed as things develop.

Before initiating live controls, survey the overall situation in an iterative fashion:

1. Identify Regulated Data to be controlled. For retail organizations, scanning for a simple combination o customer name and card ID is recommended as a starting data set to use. This set of data (though simple) will serve as a good marker for identifying PCI protected records in a scanned target. There are many methods to utilize DLP to discover where PCI related information is residing or being transmitted. For example ,detecting and preventing unencrypted PCI data in outbound communications may be applicable in many cases

Insist on a Proof of Concept demonstration done in your own environmen

2. Identify potential places where PCI information might leak. For most organizations it is recommended to inspect the following channels:
   - Email – Consider all out bound email traffic including attachments..
   - Web traffic – Gmail, and other web mail providers, Facebook and other social media sites should be monitored
   - Other protocols – In particular unencrypted communications should not be crossing the organizational firewall without first identifying the information
   - Data storage – Identify and categorize the information on all storage under control of the organization, including file servers, file shares, SAN, SharePoint servers, user home directories, workstations and laptops in order to determine the assets requiring review and inspection.
   - USB, DVD – Consider workstations that allow USB m ass storage or DVD burning and any devices that can be physically disconnected and carried away.
3. Scan data stores for PCI information. Once assets have been determined, identify any potential regulated or sensitive information on that information asset. A DLP solution will assist in this for example, as a first step, identify all files containing a customer name plus primary account number, PAN. Or a list of all users sending emails containing customer name and card ID. Or a list of all all files copied to USB devices that contain account information.
4. Review any PCI data found. Review information uncovered in step 3. Is it OK for PII to be transmitted to the destinations it is going to? In particular in the case of large transfers, is this data being encrypted and sent to known partners? Is it OK for PII to be on this network share? Is it OK for this person to send this list of PII to their email account?
5. Apply controls. Repeat these steps until a satisfactory level of understanding is developed in the form of a map to the protected information and appropriagte contols are in place and unerstood by the stakeholders and system users.

   Most organizations should expect to initially encounter lots of little potential violations such as discussing a single customers records with a banking institution, or, attempting a file upload involving all customers making purchases during the past 24 hours to a 3rd party system.

The standards cover all organizations that store, process, and transmit cardholder data, around the world

The Benefits

A major use of DLP is as the appropriate cornerstone of PCI Risk Analysis audits At an early stage, conduct a mock compliance audit. Not only will you be ready if your organization is subjected to an audit, but, it will force questions to be asked re where to focus on risk mitigation

More than a Security system, DLP is a valuable management tool once understood and properly deployed. Its benefits are centered on protecting against leaks of regulated information. However, an appropriate DLP solution may be applied to the broader context of security systems and overall policies for information governance. This is particularly the case in the management of personal financial information. The suggestions made here, in particular, those suggesting a methodical and "easy steps at a time" approach are based on years of experience working with organizations handling PCI data.

About Code Green Networks

Code Green Networks delivers solutions that help enterprises protect and manage regulated and other sensitive digital information across their data network, whether local, remote, mobile or in the cloud. The company's solutions have been tested and proven through daily use by hundreds of deployments in large and small organizations across the United States and around the globe.

It's All About The Data

Code Green's total focus is data protection utilizing innovative content inspection technology to insure maximum protection for an organization's important data. By investing over 200 man years in software development and working closely with customers since 2004, Code Green Networks has applied innovative technology to produce Data Loss Prevention solutions with the most advanced capabilities available to locate, identify and manage regulated data. Significant examples include:

A complete "Content Aware" DLP solution: TrueDLP
The Deep Inspection Content Engine: DICE
Protection extending to the cloud: Cloud Content Control

Removing Compliance Complexity

Code Green Networks believes that many products offered to address regulatory compliance are often needlessly complex in implementation and difficult to manage leading to unplanned costs and delays resulting in diminished benefits to the organization. Code Green has taken a different approach. We chose to deliver solutions that are faster to deploy, easier to manage, highly accurate with superior performance and significantly less costly than alternative solutions. Our attention to these details has produced major benefits for our customers:

Enhanced simplified management control for consistent uniform policy administration
Powerful yet simple to deploy appliances designed for quick installation
PoEasy modular growth by capacity, function and location

Committed to Supporting Our Customer's Compliance Requirements

Working with customers to address the rigorous regulations faced by organizations handling personal medical and financial information has led to our deep understanding of these particular areas of regulatory compliance. It has also helped us create solutions which are very applicable to other markets as well. We fully understand that there is no margin for error when it comes to protecting our client's critical data and this commitment to our customers guides us in everything we do.

Code Green Networks, Inc.

385 Moffett Park Drive
Suite 105
Sunnyvale, CA 94089
Phone: +1 (408) 716-4200
E-mail: info@codegreennetworks.com
www.codegreennetworks.com