NETPRO

Your IT infrastructure. Simplified.

PCI Compliance Can Make Your Organization Stronger and Fitter

Brent Harman
Manager, Systems Consultant Team West
NetPro Computing, Inc.

Today’s Agenda

- PCI DSS – What Is It?
- The Regulation
  - 6 Controls
  - 12 Requirements
- Practical Focus
  - Low hanging fruit
- More Information?

NETPRO

Solving Your Challenges

Simplify the Complexity

Lack of centralized management and rising compliance costs mean greater complexity.

Change Auditing
GLBA
Identity auditing
HELP!
E-discovery
E-mail Management
Compliance reporting
ILM Management
Exchange Migration
PCI
SOX
GPO Management
HIPAA
Recovery

PCI DSS – 30 Second Summary

Payment Card Industry (PCI)

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of industry regulations imposed by the major credit card companies to **ensure the safety, security, and integrity of cardholder data**.

- While Windows itself isn't the beginning or end of PCI compliance, it does contribute a remarkable amount to overall compliance situation when **Windows-based computers are used to store cardholder information or process credit card transactions**.

Why Comply?

- Visa fined non-compliant merchants **$4.6 million in 2006** and $3.4 million in 2005.
- Visa has announced that as of October 1, 2007 Tier 1 and Tier 2 merchants who are not in compliance with the Payment Card Industry Data Security Standard will be downgraded one tier, meaning they **will have to pay more for clearance services**.
- Additionally, Tier 1 merchants who remain noncompliant will be assessed **fines starting at $25,000 per month**.
- Visa began rewarding acquiring banks whose members were fully compliant by September 30, 2007 part of **$20 million in reward money set aside for this purpose**.

NETPRO

Have You Considered?

- It just makes good business practice to keep data secure, and the same standards should be considered in regards to securing all sensitive data.
- Adhering to PCI DSS helps companies build a more secure and efficient IT infrastructure and can actually reduce compliance costs in the long run.

Does This Apply to My Organization?

- Do you use Windows or UNIX Servers to store cardholder information or process credit card transactions?
- The Payment Card Industry Data Security Standard (PCI DSS) is a set of industry regulations imposed by the major credit card companies to ensure the safety, security, and integrity of cardholder data. Consisting of 12 requirements grouped into six control objectives, PCI DSS offers service providers and merchants a systematic way to safeguard sensitive cardholder data.

Core PCI Requirements for Windows and Active Directory®

- Any business that processes, stores, and transmits the Primary Account Number (PAN)—within the cardholder data environment—must comply with this complex new standard, and must be able to demonstrate that compliance through automated and manual audits of their systems. Systems in the cardholder data environment include any:
  - **Network** component (including, but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances).
  - **Server** (including but not limited to web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
  - **Application** (purchased and custom applications, including internal and external Internet applications).

Areas of Focus

- Breach Disclosure
- Environmental Access
  - Who has access to what?
- Strong authentication
- Restricting on the “Need to know”
- Scoping and Zoning

PCI DSS: Securing access to cardholder data

6 Controls with 12 Requirements:

- **Build and maintain a secure network**
  - 1. Install and maintain a firewall configuration to protect data.
  - 2. Change vendor-supplied defaults for system passwords and other security parameters.
- **Protect cardholder data**
  - 3. Protect stored cardholder data.
  - 4. Encrypt transmissions of cardholder magnetic-stripe data and sensitive information across public networks.
- **Maintain a vulnerability management program**
  - 5. Use and regularly update anti-virus software.
  - 6. Develop and maintain secure systems and applications.
- **Implement strong access controls**
  - 7. Restrict access to cardholder data to a need-to-know basis. .
  - 8. Assign a unique ID to each person with computer access.
  - 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.

The Details

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.
   - 2.2.4. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
   - 6.1. Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

The Details, cont.

7. Restrict access to cardholder data by business need-to-know.
   - 7.1. Limit access to computing resources and cardholder information only to those individuals whose job requires such access.
8. Assign a unique ID to each person with computer access.
   - 8.5.1. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
   - 8.5.9. Change user passwords at least every 90 days
   - 8.5.10. Require a minimum password length of at least seven characters
   - 8.5.13. Limit repeated access attempts by locking out the user ID after not more than six attempts
9. Restrict physical access to cardholder data.

NETPRO

And More Details…

10. Track and monitor all access to network resources and cardholder data.

  - 10.1. Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user
  - 10.2. Implement automated audit trails for all system components to reconstruct the following events:
    - 10.2.1. All individual user accesses to cardholder data
    - 10.2.2. All actions taken by any individual with root or administrative privileges
    - 10.2.3. Access to all audit trails
    - 10.2.4. Invalid logical access attempts
    - 10.2.5. Use of identification and authentication mechanisms
    - 10.2.6. Initialization of the audit logs
    - 10.2.7. Creation and deletion of system-level objects.
  - 10.3. Record at least the following audit trail entries for all components for each event:
    - 10.3.1. User identification
    - 10.3.2. Type of event
    - 10.3.3. Date and Time
    - 10.3.4. Success of failure indication
    - 10.3.5. Origination of event
    - 10.3.6. Identity or name of affected data, system component, or resource
  - 10.5.1. Limit viewing of audit trails to those with a job related need.
  - 10.5.2. Protect audit trails files from unauthorized modifications

Details, the rest…

10. Track and monitor all access to network resources and cardholder data.
    - 10.5.3. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
    - 10.5.4. Copy logs for wireless networks onto a log server on the internal LAN.
    - 10.5.5. Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
    - 10.6. Review logs for all system components at least daily. Logs review must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (e.g. RADIUS)
    - 10.7. Retain audit trail history for at least one year, with a minimum of three months available online.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security

PCI Customer Stories

- **National Grocery Store Chain**
  - Auditors are not only looking for assurance that they have controls in place, they want proof
  - Auditors required the ability to actively report on when staff is added or removed from the admin groups and when a Group Policy Object is added or modified.
  - Needed the ability to report on system access right down to the file level with exception reports that highlight when users access files that are not their own.
- **Major Clothing Retailer**
  - Required to show proof that no disabled accounts existed, and that disabled accounts were being deleted in a timely fashion
  - Found they needed to watch for administrators creating duplicate accounts in order to “hide” improper access to cardholder data.
  - By providing irrevocable, irrefutable logs collected in real-time that covered every operation in Active Directory, the retailer was able to satisfy auditors with virtually no administrative overhead.

Top 10 Things to Show the Auditor

1. Who has access to a specified file or other resource?
2. Who has had access to a given file or other resource in the past?
3. What resources does a given individual have access to across your entire enterprise.
4. Proof that password policies and other directory settings are correct and have remained so over time.
5. Proof that inactive accounts were deleted within the allowed timeframe.
6. Proof that duplicate accounts do not exist.
7. Proof that account removal, modification, and addition is performed according to policies and requirements.
8. What security settings are currently in effect in your environment?
9. What security settings have been in effect in your environment in the past?
10. That security settings are consistently applied throughout the environment.

PCI Compliance Checklist for Your Entire Enterprise

Can you show?

- ❑ Who has access to a specified file or other resource?
- ❑ Who has had access to a given file or other resource in the past?
- ❑ What resources a given individual has access to across your entire enterprise?
- ❑ That password policies and other directory settings are correct and have remained so over time?
- ❑ That inactive accounts were deleted within the allowed timeframe?
- ❑ That duplicate accounts do not exist?
- ❑ That account removal, modification, and addition is performed according to policies and requirements?
- ❑ What security settings are currently in effect in your environment?
- ❑ What security settings have been in effect in your environment in the past?
- ❑ That security settings are consistently applied throughout the environment?
- ❑ What changes have been made to security settings over time?
- ❑ What privileges have been exercised by users, particularly administrative users?
- ❑ What privileges have been exercised by users, particularly administrative users?
- ❑ Audit logs with all access by all users to all resources?
- ❑ Audit logs with all actions taken by administrators?
- ❑ Audit logs with all access to auditing information?
- ❑ Audit logs with all invalid access attempts?
- ❑ Audit logs with all use of authentication mechanisms such as Active Directory?
- ❑ Audit logs with all initialization (clearing) of audit logs?
- ❑ Audit logs with all creation and deletion of system-level objects?
- ❑ Proof that all systems are up-to-date with the latest service releases?
- ❑ That you can detect unpatched systems and either correct the problem or alert an administrator to do so?
- ❑ That the correct policies are in place to ensure secure transmission of cardholder data?
- ❑ That secure transmission policies have remained in effect continuously?

NETPRO

Lessons Learned

- Auditing is absolutely key moving forward
- Wireless access compliance is becoming more prominent
- Group Policy (through AD) is a key process for ensuring that access is locked down.
- There are aspects of compliance that cannot be traced today, specifically web application login. They will have to be audited in the future.
- Legacy systems are a major issue because they store more information than they should (because compliance wasn’t a concern when they were developed in the early 90’s.)

NETPRO

Other Things to Consider

- Watch for changes in PCI regulations in coming years. Next changes could be major or minor – it’s hard to say right now.
- There is a rolling interest/adoption of PCI regulations/standards in other parts of the world. International standards currently lag behind, but this will change over time.

Example Reports and Forms

TABLE OF CONTENTS

Demonstrating PCI Complia

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.	SecurityManager provides real-time compliance monitoring to detect when any systems are out of compliance.		
3. Protect stored cardholder data.	AccessManager provides a central role-based model to define, deploy, enforce, and report against access to systems and critical files.	SecurityManager pr monitoring of Active memberships and e duties on these grou to grant access to app	
4. Encrypt transmission of cardholder data across open, public networks.	SecurityManager monitors compliance of server settings such as IPSEC policies to ensure that they are properly configured.		
5. Use and regularly update anti-virus software.	SecurityManager monitors compliance of server settings such as service pack levels to ensure that they are properly configured.		
6. Develop and maintain secure systems and applications.	SecurityManager ensures that approved server configurations are actually rolled out manually or through group policy to secure the Windows environment. Then it tracks changes to hot fixes or service packs to ensure that systems are properly hardened.		
7. Restrict access to cardholder data by business need-to-know.	AccessManager encourages least privilege use as roles a to fulfill their job functions. Access can also be granted for remove permissions that are no longer appropriate. Lastly what resources within the organization.		
8. Assign a unique ID to each person with computer access	NetPro can track any new user accounts in Active Directo track changes to these accounts in real time and provide a		
9. Restrict physical access to cardholder data.	NetPro can help with a lot…unfortunately not this one!		
10. Track and monitor all access to network resources and cardholder data.	ChangeAuditor tracks all changes to Active Directory, Exchange, and file system data. ChangeAuditor also tracks user activity including logins, failed logins, file access, access attempts, etc.		
11. Regularly test security systems and processes.	NetPro prevents security breaches and vulnerabilities by automating remediation of security configurations.	NetPro provides a dashboard highlig risk areas across Active Directory.	determined intervals.
12. Maintain a policy that addresses information security.	NetPro real-time compliance identifies inappropriate or unapproved server and Active Directory changes. Combined with real-time auditing, NetPro can be used to isolate suspect activity and identify the root cause of compliance violations down to the specific user and specific change. Providing before and after values allows administrators to immediately restore systems to their last "known and trusted" state.		

Is your organization ready to face a PCI audit?

Use this PCI auditing checklist to see if you're ready and to determine what your auditor will want to see as it relates to Microsoft Windows and Active Directory. Remember, you must be able to prove compliance for your entire enterprise, not just individual servers.

Can you show…?

- □ Who has access to a specified file or other resource?
- □ Who has had access to a given file or other resource in the past?
- □ What resources a given individual has access to across your entire enterprise?
- □ That password policies and other directory settings are correct and have remained so over time?
- □ That inactive accounts were deleted within the allowed timeframe?
- □ That duplicate accounts do not exist?
- □ That account removal, modification, and addition is performed according to policies and requirements?
- □ What security settings are currently in effect in your environment?
- □ What security settings have been in effect in your environment in the past?
- □ That security settings are consistently applied throughout the environment?
- □ What changes have been made to security settings over time?
- □ What privileges have been exercised by users, particularly administrative users?
- □ Audit logs with all access by all users to all resources?
- □ Audit logs with all actions taken by administrators?
- □ Audit logs with all access to auditing information?
- □ Audit logs with all invalid access attempts?
- □ Audit logs with all use of authentication mechanisms such as Active Directory?
- □ Audit logs with all initialization (clearing) of audit logs?
- □ Audit logs with all creation and deletion of system-level objects?
- □ Proof that all systems are up to date with the latest service releases?
- □ That you can detect unpatched systems and either correct the problem or alert an administrator to do so?
- □ That the correct policies are in place to ensure secure transmission of cardholder data?
- □ That secure transmission policies have remained in effect continuously?

Ideally, auditors should be able to access these items through the self-service, Web-based reporting mechanism found in NetPro. Auditors can pull the information they need to complete their audit—imposing no administrative overhead on you and your staff.

NetPro speeds PCI compliance, making audits easier to pass and removing administrative overhead from your IT staff.

www.netpro.com

Assets Available to Download

- Core PCI Requirements Whitepaper
- PCI Sample Reports
- PCI Compliance Grid
- Audit Checklist

NETPRO

We Got Your Back

Need More?:

- •PCI White Paper: Core PCI Requirements for Windows & AD
- •PCI Audit Checklist: PCI Auditing Checklist for Windows & AD
- •PCI Compliance Grid: How NetPro helps with Windows-Related PCI Compliance
- •PCI Report Book: Key NetPro PCI Reports

http://www.netpro.com/go/PCI

NETPRO

TEC 2009 for Directory & Identity and Exchange

- **Join NetPro and Microsoft for the ONLY conferences**
- **for expert training on Microsoft Directory & Identity**
- **and Exchange Technologies!**

- **Dedicated Conferences for Directory & Identity and Exchange**
- **In-Depth, Highly Technical Content**
- **One-on-one Access to Microsoft Technology Leaders**
- **Invaluable Networking Opportunities**

- **Registration opens Aug. 25!**

Las Vegas - March '09

The Experts Conference

www.tec2009.com

Berlin - September '09

NETPRO

Your IT infrastructure. Simplified.

Questions?

Brent Harman

bharman@netpro.com