



PERCONA  
Performance Consulting Experts

---

# Achieving PCI Compliance with MySQL

Ryan Lowe & Fernando Ipar  
2010 O'Reilly MySQL C&E

# Agenda

- Overview of PCI
- Which requirements apply to us?
- Requirement-by-requirement discussion
- Questions

# PCI DSS

- History
- Goals
- Common Myths

# Merchant Responsibility

Merchant Level	Definition	Requirements
1	6M+	Annual Audit Quarterly Network Scan **
2	1M-6M	Quarterly Network Scan ** V: Annual Self-Assessment *** M: Annual Audit (QSA)
3	20k-1M	Quarterly Network Scan ** Annual Self-Assessment ***
4	<20k	Quarterly Network Scan ** Annual Self-Assessment *

\* Recommended

\*\* Qualified Independent Scan Vendor

\*\*\* Merchant

# PCI DSS v1.2

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

NETWORK SECURITY

DATA SECURITY

PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

NETWORK SECURITY

DATA SECURITY

PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

NETWORK SECURITY

DATA SECURITY

PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CARD  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

NETWORK SECURITY

DATA SECURITY

PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

NETWORK SECURITY

DATA SECURITY

PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CARD  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 2  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CND  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

## REQ 12 MAINTAIN AN INFORMATION SECURITY POLICY

### NETWORK SECURITY

### DATA SECURITY

### PHY

REQ 1  
FIREWALL

REQ 3  
PASSWORD

REQ 4  
NETWORK  
ENCRYPTION

REQ 6  
SECURE  
SYSTEMS

REQ 11  
TESTING

REQ 2  
PASSWORD

REQ 3  
CARD  
PROTECTION

REQ 5  
ANTI-VIRUS

REQ 7  
ACCESS  
CONTROL

REQ 8  
IDENTITY

REQ 11  
TESTING

REQ 9  
PHYSICAL  
ACCESS  
CONTROL

## REQ 10 LOG MANAGEMENT

# Requirement 2

## **Do not use vendor-supplied defaults for system passwords and other security parameters**

“Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.”

# Requirement 2

```
mysql> SELECT user, host, password FROM mysql.user;
```

```
+-----+-----+-----+  
| user | host      | password |  
+-----+-----+-----+  
| root | localhost |          |  
| root | testbox1  |          |  
| root | 127.0.0.1 |          |  
|      | localhost |          |  
|      | testbox1  |          |  
+-----+-----+-----+
```

```
5 rows in set (0.28 sec)
```

# Requirement 2

```
%> mysql_secure_installation
...
Set root password? [Y/n] Y
...
Remove anonymous users? [Y/n] Y
...
Disallow root login remotely? [Y/n] Y
...
Remove test database and access to it? [Y/n] Y
...
Reload privilege tables now? [Y/n] Y
...
```

# Requirement 2

```
mysql> SELECT user, host, password FROM mysql.user;
```

user	host	password
root	localhost	*F169C0AFEEC30BFF924130B124E6AE3E875D5F60

1 row in set (0.00 sec)

```
mysql> SHOW GLOBAL VARIABLES LIKE 'old_passwords';
```

Variable_name	Value
old_passwords	OFF

1 row in set (0.00 sec)

# Password Hash is NOT Secure

```
%> strings user.MYD  
localhost  
root*F169C0AFEEC30BFF924130B124E6AE3E875D5F60  
%>
```

- Permissions for datadir, tmpdir, etc

# Requirement 2

## 2.2.3 – Configure system security parameters to prevent misuse

- Be judicious with your GRANTS
- Disable local\_infile
- Disable old\_passwords
- Set read\_only=ON
- Enable secure\_auth

# Requirement 3

## Protect Stored Cardholder Data

“Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person...”

# Requirement 3 – Data

Data Element	Storage Permitted	Protection Required	Req 3.4
Primary Account Number	Yes	Yes	Yes
Cardholder Name	Yes	Yes	No
Service Code	Yes	Yes	No
Expiration Date	Yes	Yes	No
Full Magnetic Stripe Data	No	N/A	N/A
CAV2/CVC2/CVV2/CID	No	N/A	N/A
PIN/PIN Block	No	N/A	N/A

# Requirement 3

## MySQL Encryption Functions

“ENCRYPT”	“DECRYPT”
AES_ENCRYPT()	AES_DECRYPT()
COMPRESS()	UNCOMPRESS()
ENCODE()	DECODE()
DES_ENCRYPT()	DES_DECRYPT()

One-Way Functions
ENCRYPT()
MD5()
SHA() & SHA1()
OLD_PASSWORD()
PASSWORD()

# Requirement 3 - Example

```
mysql> CREATE TABLE `cc_info` (  
-> `id` int unsigned NOT NULL auto_increment,  
-> `cc_num` varbinary(32) NOT NULL,  
-> `service_code` varbinary(32) NOT NULL,  
-> `name_on_card` varbinary(48) NOT NULL,  
-> PRIMARY KEY (`id`))  
-> ENGINE=InnoDB;
```

Query OK, 0 rows affected (0.01 sec)

$(16 * (\text{CEILING}(\text{string\_length}/16) + 1))$

# Requirement 3 - Example

```
mysql> INSERT INTO `cc_info`  
-> (`cc_num`, `service_code`, `name_on_card`)  
-> VALUES (  
-> AES_ENCRYPT('1234123412341234', 'secret_key'),  
-> AES_ENCRYPT('1234', 'secret_key'),  
-> AES_ENCRYPT('John Doe', 'secret_key'));
```

Query OK, 1 row affected (0.35 sec)

# Requirement 3 - Example

```
mysql> SELECT id, cc_num, service_code, name_on_card  
-> FROM cc_info\G
```

```
***** 1. row *****
```

```
id: 1
```

```
cc_num: ??
```

```
? q$?!~c?3Pg?"xu&3?:?,am?
```

```
service_code: y.??A??
```

```
?? ?a??
```

```
name_on_card: ?93s?!? X?8?|nZ
```

```
1 row in set (0.00 sec)
```

# Requirement 3 - Example

```
mysql> SELECT id,  
-> AES_DECRYPT(`cc_num`,`secret_key`)  
-> AS `cc_num`,  
-> AES_DECRYPT(`service_code`, 'secret_key')  
-> AS `service_code`,  
-> AES_DECRYPT(`name_on_card`, 'secret_key')  
-> AS `name_on_card` -> FROM `cc_info`\G ***** 1. row  
*****  
  
id: 1  
cc_num: 1234123412341234  
service_code: 1234  
name_on_card: John Doe  
1 row in set (0.00 sec)
```

# Requirement 3 – The Binary Log

```
%> mysqlbinlog log-bin.000001
```

```
...
```

```
#100406 16:35:31 server id 1 end_log_pos 461 Query thread_id=1  
  exec_time=0 error_code=0
```

```
use cc/*!*/;
```

```
SET TIMESTAMP=1270596931/*!*/;
```

```
INSERT INTO `cc_info` (`cc_num`, `service_code`, `name_on_card`)  
  VALUES (AES_ENCRYPT('1234123412341234', 'secret_key'),  
  AES_ENCRYPT('1234', 'secret_key'), AES_ENCRYPT('John Doe',  
  'secret_key'))
```

```
# at 461 #100406 16:35:31 server id 1 end_log_pos 488 Xid = 6
```

# Requirement 3 – The Binary Log

```
%> mysqlbinlog -v log-bin.000001
...
BINLOG '
Msa7SxMBAAAANQAAAN0DAAAAAA8AAAAAAAmNjAAAdjY19pbmZvAAQD/g8PBv4gIAA
wAAA=
Msa7SxcBAAAAZQAAAEIEAAAQAA8AAAAAAEABP/wBAAAACCY3AusAHEkreUIIX5jyzNQ
Z90ieHUm
M8Y6BgflLGFtjxB5Lo7nQeK6zQr+wQCVYabiELI5M3P+IYoAWOo4iHxuWhl=
'/*!*/;
### INSERT INTO cc.cc_info
### SET
### @1=1
### @2='??\x0b?\x00q$??\x08!~c?3Pg?"xu&3?:\x06\x07?,am?'
### @3='y.??A??\x0a??\x00?a??'
### @4='?93s?!?\x00X?8?|nZ\x12'
# at 1090 #100406 16:39:30 server id 1 end_log_pos 1117 Xid = 23 COMMIT/*!*/
```

# Requirement 3 – Alternatives

- Full Disk Encryption
  - Logical access must be managed independently of native operating system access control mechanisms
- Encrypt in the Application Layer
  - Key Handling & Management Issues

# Requirement 3 – Additional

- 3.1 – Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
- 3.2 – Do not store sensitive authentication data after authorization (even if encrypted).
- 3.3 – Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

**Don't Forget Your Backups**

# Requirement 4

## **Encrypt transmission of cardholder data across open, public networks**

- The traffic between datacenters is encrypted at the network layer (secure VPN, for example)
- Applicable data is encrypted before being inserted into the database (encrypting in the application layer or using RBR).
- You use MySQL Replication over SSL

# Requirement 6

## **Develop and maintain secure systems and applications**

“...All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.”

# Requirement 6 - Overview

- Validation of all input
- Validation of proper error handling
- Validation of secure cryptographic storage
- Validation of secure communications
- Separate development/test and production environments
- Separation of duties between development/test and production environments
- Production data (live PANs) are not used for testing or development
- Web Application Security (XSS, CSRF, etc)
- Formalizing the process for security updates

# Requirement 6

- 6.2 - Establish a process to identify newly discovered security vulnerabilities
  - BugTraq
  - MySQL Announce List
- 6.4 – Follow change control procedures for all changes to system components
  - Documentation of impact
  - Management sign-off by appropriate parties
  - Testing of operational functionality
  - Back-out procedures

# Requirement 7

## **Restrict access to cardholder data by business need to know**

- **VIEWS are your friend**
- **Follow Account Best Practices**
  - Requirement 2

# Requirement 7 – Resource Limits

- MAX\_QUERIES\_PER\_HOUR
- MAX\_UPDATES\_PER\_HOUR
- MAX\_CONNECTIONS\_PER\_HOUR
- MAX\_USER\_CONNECTIONS

# Requirement 8

## **Assign a unique ID to each person with computer access**

- Assign all users a unique ID before allowing them to access system components or cardholder data
- Ensure proper user authentication and password management for non- consumer users and administrators on all system components

# Requirement 10

## **Track and monitor all access to network resources and cardholder data**

- Establish a process for linking all access to system components to each individual user
- Implement automated audit trails for all system components to reconstruct events
- Record audit trail entries for all system components
- Synchronize all critical system clocks and times
- Secure audit trails so they cannot be altered
- Review logs for all system components at least daily
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

# Requirement 10 – SANS Top 5

- 1 Attempts to Gain Access through Existing Accounts
- 2 Failed File or Resource Access Attempts
- 3 Unauthorized Changes to Users, Groups and Services
- 4 Systems Most Vulnerable to Attack
- 5 Suspicious or Unauthorized Network Traffic Patterns

# Requirement 11

## **Regularly test security systems and processes**

“Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.”

# Requirement 12

## **Maintain a policy that addresses information security for employees and contractors**

- 12.1 - Establish, publish, maintain, and disseminate a security policy
- 12.2 - Develop daily operational security procedures that are consistent with requirements in this specification
- 12.3 - Develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors
- 12.4 - Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors

# Requirement 12 – Continued

- 12.5 - Assign to an individual or team security management responsibilities
- 12.6 - Implement a formal security awareness program to make all employees aware of the importance of cardholder data security
- 12.7 - Screen potential employees prior to hire to minimize the risk of attacks from internal sources
- 12.8 - If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers
- 12.9 - Implement an incident response plan. Be prepared to respond immediately to a system breach

# Ten Common Myths of PCI DSS

- 1 One vendor and product will make us compliant
- 2 Outsourcing card processing makes us compliant
- 3 PCI compliance is an IT project
- 4 PCI will make us secure
- 5 PCI is unreasonable; it requires too much
- 6 PCI requires us to hire a QSA
- 7 We don't take enough credit cards to be compliant
- 8 We completed an SAQ so we're compliant
- 9 PCI makes us store cardholder data
- 10 PCI is too hard

# Conclusions

Questions

Comments

War Stories