



PCI DSS Compliance the Rocky Road

Colin Dixon
Head of Risk and
Compliance

Planning is everything

If you don't know where you're going, you'll wind up somewhere else

Yogi Berra

Agenda

- Approaches to the standard
- Problems with getting underway
- Some major issues and how we fixed them
- Your questions answered

The major issues with PCI DSS compliance programmes

- Viewed as an IT issue
- No clear visibility or ownership within the business
- Lack of focus from senior management
- Compliance expected from within existing IT budgets
- Difficult or impossible to get additional funding
- Little or no audit focus
- Risks not understood

PCI DSS is a continuing commitment

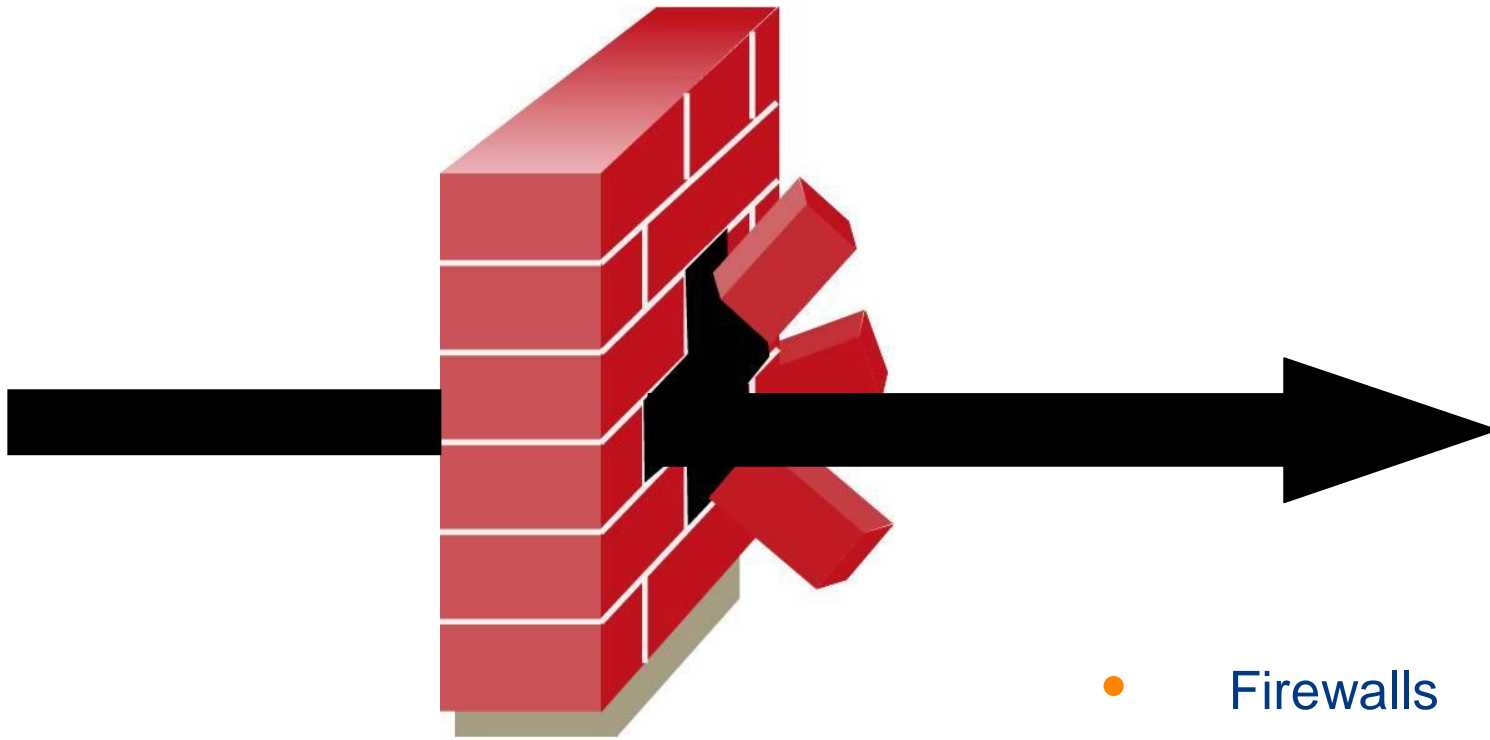
- PCI DSS compliance needs:
- Responsibility and authority from within the business
- Clearly set out within the structure of the business
- Realistic budget based on business need
- Focus within the business
- Continuity



Governance and compliance structures

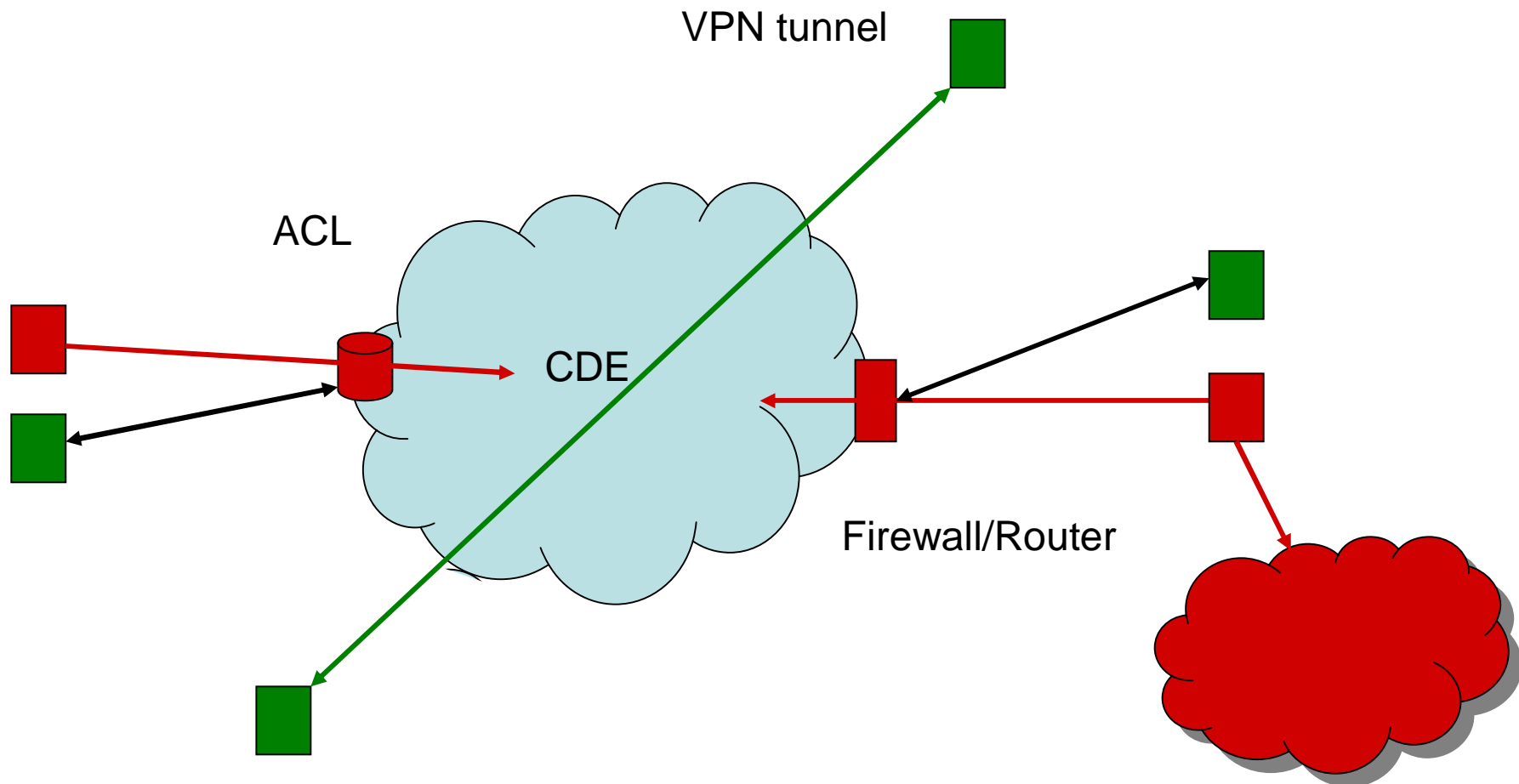
- Include in existing risk structure
- Highlight cost of losing the transaction channel
- Include in the company risk register
- Include in the top 10 corporate governance risks
- Integrate into the risk reporting structure
- Establish a programme with a director sponsor

Network Segmentation and the contamination rule



- Firewalls
- Routers
- ACLs
- Subnets

Network Segmentation and the Contamination Rules



Cardholder Data Proliferation

- Discovery
- Identification
- Sell-by date
- Destruction
 - Shredding
 - Sanitising
 - Secure storage
 - Encryption



Cardholder Data retention and destruction

- Policy
- Secure deletion
- Archives
- Deleting free space
- Application space
- Paper
- Old disks etc.



PCI DSS and Call Centres

- Analogue
- Digital
- Archives
- Paper etc.

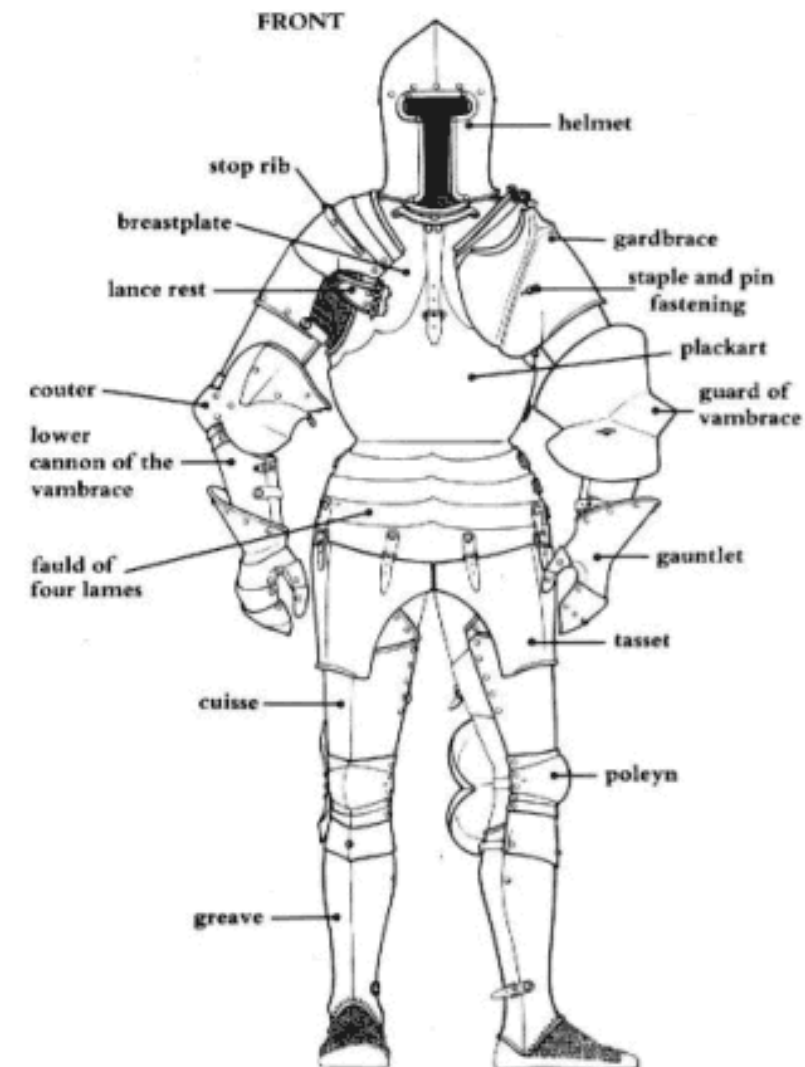
Solutions

- **IVR**
- Key entry
- Integrated applications
- Data sanitisation



Networks

- Secure build standards
- Wireless policy + scans
- WPA2 for wireless
- Change management



Testing and scanning

- Quarterly external quarterly scans for vulnerabilities
- Quarterly internal quarterly scans for vulnerabilities
- Annual penetration test of
 - Network internal and external
 - Application internal and external
- Application code review or application firewall for Web facing applications

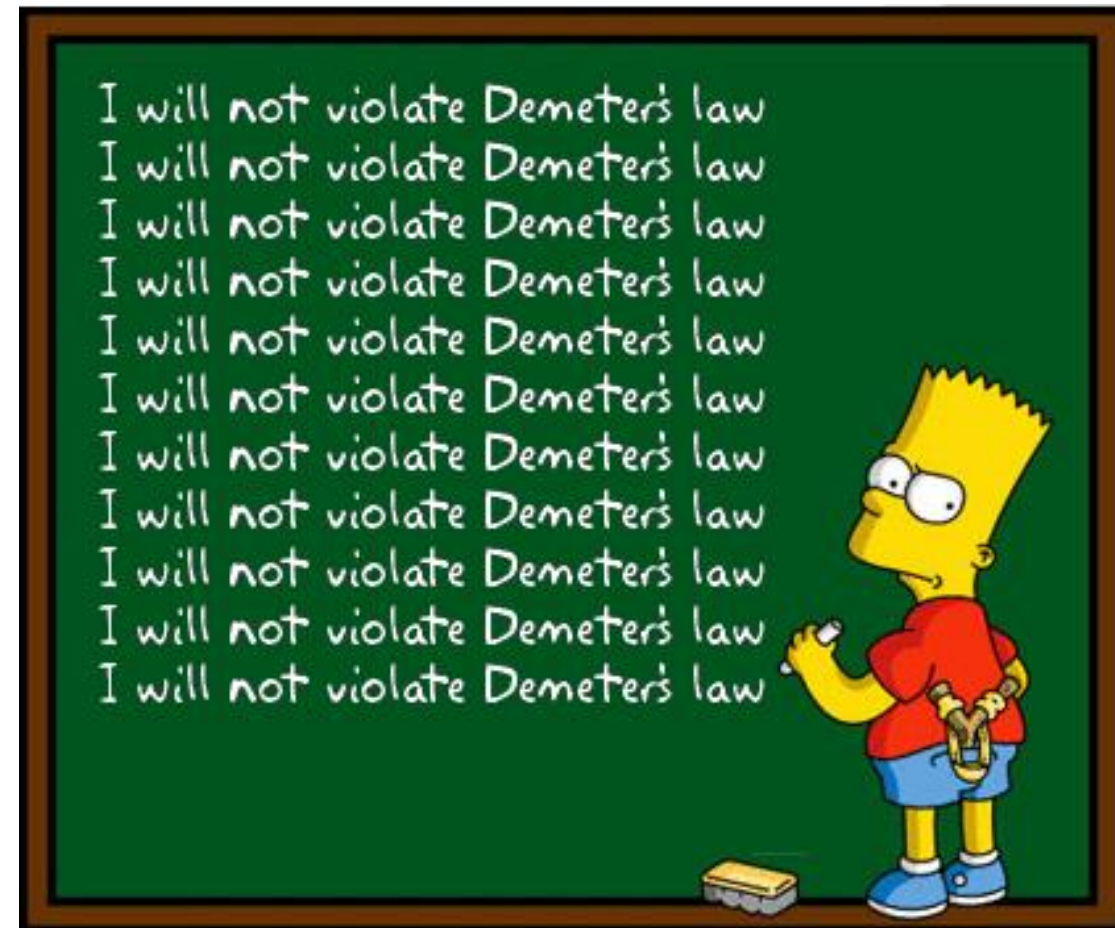


Individual Accountability

- Unique ID
- Password or two factor
- Two factor for remote access
- No:
 - Sharing of user ID's
 - Sharing of passwords
 - Sharing of access codes/ tokens

Application Design and Development

- Design standards
- Development policy
- PA-DSS
- Testing
- Token based solution



Backups and recovery

- Encrypt cardholder data on backups
- Store media back-ups in a secure location
- Secure courier to off-site
- Destruction of stored data
- Inventory logs of stored media



Incident management

- Incident management system to ensure timely and effective handling of all situations including:
 - Incident response plan
 - Annual testing
 - Named individuals responsible
 - Trained operators
- Include alerts from
 - intrusion detection
 - intrusion prevention
 - file integrity monitoring
- Incident policy and procedure



Information risk management

- Information security policy
- Risk analysis and management
- Allocation of responsibilities
- Daily operational security procedures
- Usage policies for:
- Control of access by third parties
- Written agreement with service providers
- Monitor service provider's compliance



Formal Policies and Procedures

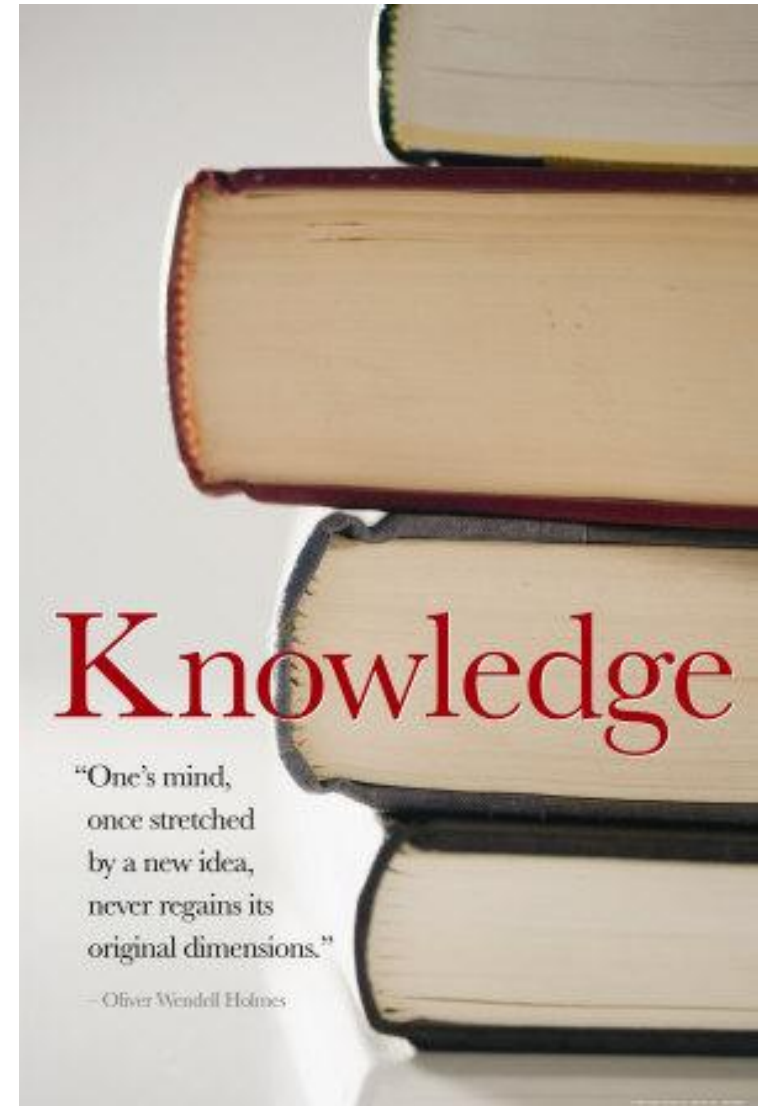
- Four areas of compliance:
 - Policies
 - Standards
 - Procedures
 - Awareness



P O L I C I E S

Employee awareness of the need to protect cardholder data

- List of all employees with access to cardholder data
- Vetting on employment (CRC etc.)
- Awareness information on joining
- Annual signing of the information security policy
- Annual awareness building programme



Planning is Everything





Questions?

Colin.dixon@mwrinfosecurity.com